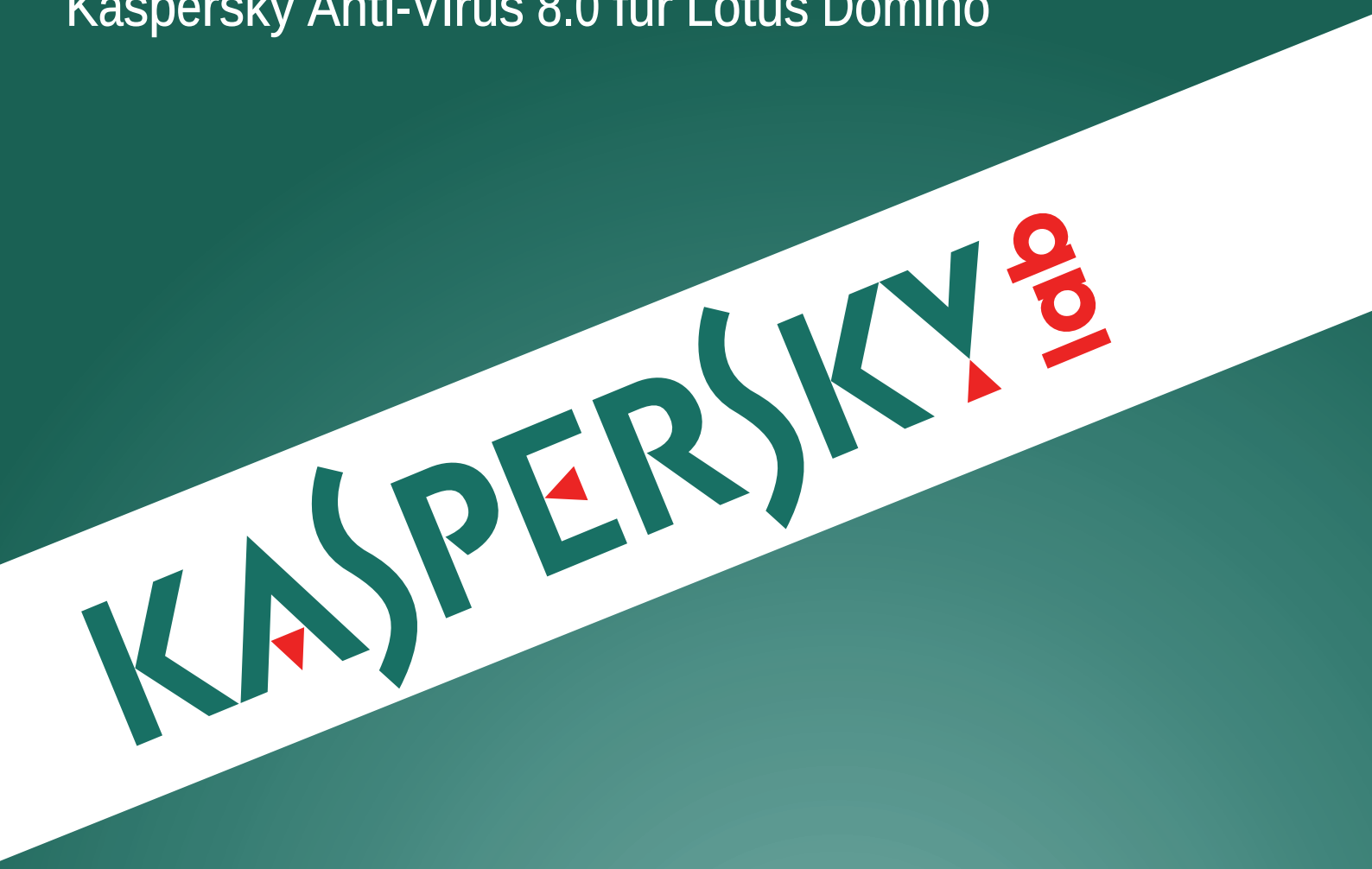
Kaspersky Anti-Virus 8.0 für Lotus Domino



Administrator-handbuch

PROGRAMMVERSION: 8.0

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass Ihnen dieses Dokument bei Ihrer Arbeit hilft und die meisten aufkommenden Fragen beantwortet.

Wichtiger Hinweis: Die Rechte an diesem Dokument liegen bei der Kaspersky Lab GmbH und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt. Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach den Gesetzen der Russischen Föderation zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Vervielfältigen in jeglicher Form und das Weiterverbreiten der Unterlagen, unter anderem auch in übersetzter Form, ist nur nach vorheriger schriftlicher Genehmigung der Kaspersky Lab GmbH zulässig.

Das Dokument und die dazugehörigen Grafiken dürfen nur zu informativen, nicht kommerziellen und persönlichen Zwecken verwendet werden.

Änderungen des Dokuments ohne vorherige Ankündigung bleiben vorbehalten. Die jeweils neueste Version des Dokuments finden Sie auf der Webseite von Kaspersky Lab unter der Adresse http://www.kaspersky.de/docs.

Kaspersky Lab ZAO übernimmt keine Haftung für den Inhalt, die Qualität, die Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, die das Eigentum anderer Rechtsinhaber sind, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechtsinhaber sind.

Datum der Dokumentredaktion: 09.12.2010

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

www.kaspersky.de
http://support.kaspersky.de

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN" KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

WENN DIE SOFTWARE MIT EINEM LIZENZVERTRAG ODER EINEM VERGLEICHBAREN DOKUMENT GELIEFERT WIRD, SIND DIE BEDINGUNGEN DER SOFTWARE-NUTZUNG GEMÄSS EINEM SOLCHEN DOKUMENT GEGENÜBER DIESEM ENDNUTZER-LIZENZVERTRAG MASSGEBEND.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE „AKZEPTIEREN" GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie"* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation"* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung

2.1. Sie erhalten hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung") der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz"). Sie erkennen diese Lizenz an.
Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Computer, die in den Lizenzen festgelegt ist, die Sie bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software erworben haben.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.

2.5. Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Erwerbs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.

3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.

3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Erwerbs bezeichnete Zeitdauer genutzt werden.

3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt.

3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.

3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.

3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.

3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

4. Technische Unterstützung

4.1. Die in Klausel 2.5 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).

Technischer Support: http://support.kaspersky.com

4.2. Die Daten des Benutzers, wie in Personal Cabinet/My Kaspersky Account festgelegt, können von den Experten vom Technischen Support nur während der Bearbeitung des Antrags des Benutzers verwendet werden.

5. Beschränkungen

5.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

5.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen.

5.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet.

5.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

5.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.

5.6. Ihre Schlüsseldatei kann blockiert werden, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen.

5.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

6. Eingeschränkte Garantie und Haftungsausschluss

6.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

6.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

6.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

6.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.5 dieses Vertrags erläutert, Updates herunterladen.

6.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.

6.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU

ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

7. Haftungsausschluss und Haftungsbeschränkungen

7.1. INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS UND/ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER UND/ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

8. GNU und sonstige Drittpartei-Lizenzen

8.1. Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software"). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

9. Geistiges Eigentum

9.1. Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze

zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken"). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

9.2. Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

10. Geltendes Recht; Schiedsverfahren

10.1. Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 10 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

11. Zeitraum für Rechtsverfolgung.

11.1. Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

12. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

12.1. Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

13. Kontaktinformationen des Rechtsinhabers.

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

INHALT

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE 3

ÜBER DIESES HANDBUCH 12

- In diesem Dokument 12
- Kennzeichnungen 14

ZUSÄTZLICHE INFORMATIONSQUELLEN ÜBER DAS PROGRAMM 15

- Informationsquellen zur selbständigen Recherche 15
- Anfrage an die Vertriebsabteilung 16
- Anfrage an die Dokumentationsentwicklungsgruppe 16
- Beurteilung von Kaspersky Lab Programmen im Webforum 16

KASPERSKY ANTI-VIRUS 8.0 FÜR LOTUS DOMINO 17

- Was gibt es Neues 18
- Lieferumfang 19
- Service für registrierte Benutzer 19
- Hard- und Softwarevoraussetzungen 19

PROGRAMM-ARCHITEKTUR 21

- Schema des Anti-Viren-Serverschutzes 22
  - Schema des Programmablaufs 23
  - Anti-Viren-PrüfAlgorithmus 24
  - Algorithmus zur Filterung von Anhängen 24
  - Verarbeitung der Objekte und auf sie angewandte Aktionen 25
- Kaspersky Anti-Virus Einstellungsverwaltung 26
- Einstellungsverwaltung der Konfigurationsdatei notes.ini 28
- Berechtigungsverwaltung 30
  - Berechtigungsverwaltung auf ACL Ebene der Kaspersky Anti-Virus Datenbanken 30
  - Berechtigungsverwaltung auf Ebene der Profil- / Serverparameter 33

LIZENZVERWALTUNG 34

- Über den Lizenzvertrag 34
- Über die Kaspersky Anti-Virus-Lizenzen 35
- Über die Kaspersky Anti-Virus-Schlüsseldatei 35
- Installation der Schlüsseldatei 36

PROGRAMMOBERFLÄCHE 38

- Fensterstruktur der Verwaltungscenter Datenbank 40
- Schutzverwaltung Tab 41
- Ereignisprotokoll und Statistik Tab 44
- Hilfe Tab 45

PROGRAMM STARTEN UND BEENDEN 46

SERVERSCHUTZZUSTAND 47

STANDARDMÄßIGER SERVERSCHUTZ 49

UPDATE DER DATENBANKEN 51

- Updatequelle 52
- Update-Schema 53
- Updatequelle auswählen 55

Planmäßiges Update 56
Manuelles Update 58
E-MAIL-SCHUTZ 59
E-Mail-Schutz aktivieren und deaktivieren 60
Auswahl von Objekten des E-Mail-Schutzes 61
Aktionen an den E-Mail-Objekten 62
Filtern von E-Mail-Anhängen 67
Benachrichtigungen über Epidemien 68
REPLIKATIONSSCHUTZ 71
Replikationsschutz aktivieren / deaktivieren 72
Auswahl von Objekten des Replikationsschutzes 73
Aktionen für Objekte im Modus des Replikationsschutzes 74
Filtern von Anhängen im Modus des Replikationsschutzes 76
UNTERSUCHUNG DER DATENBANKEN 78
Untersuchung der Datenbanken aktivieren und deaktivieren 79
Auswahl von Objekten der Datenbankenüberprüfung 80
Aktionen für Objekte im Modus der Datenbankenüberprüfung 82
Filtern von Dateianhängen im Modus der Datenbankenüberprüfung 84
Planmäßige Untersuchung 86
Manuelle Untersuchung 87
LEISTUNG 89
QUARANTÄNE 91
Einsicht der in die Quarantäne verschobenen Objekte 92
Aktionen an den in die Quarantäne verschobenen Objekte 94
Quarantäne-Einstellungsanpassung 96
EREIGNISPROTOKOLL UND STATISTIK 98
Einstellungen des Ereignisprotokolls 99
Statistikeinstellungen 101
Löschen der Information aus der Ereignisprotokoll- und Statistikdatenbank 104
Die Ereignisprotokoll- und Statistikdatenbank einsehen 105
Allgemeines Ereignisprotokoll und Statistik einsehen 105
Ereignisprotokoll und Statistik für einen Server durchsehen 107
BENACHRICHTIGUNGEN 109
KONFIGURATIONSVERWALTUNG 112
Profile erstellen und löschen 112
Einsetzung vom Profiladministrator 114
Einsetzung vom Serveradministrator 114
Server zu einem anderen Profil verschieben 115
Anpassung der einzelnen ServerEinstellungswerte 115
Verwendung der Option der direkten Bearbeitung der Servereinstellungen 118
ÜBERPRÜFUNG DER PROGRAMMEINSTELLUNGEN AUF RICHTIGKEIT 119
Test "virus" EICAR und seine Modifikationen 119
Testen des E-Mail-Schutzes 120
Testen des Replikationsschutzes 121
Testen der Datenbankenuntersuchung 121

SERVER-KONSOLE-MODUS 122
ANFRAGE AN DEN TECHNISCHEN SUPPORT 124
GLOSSAR 125
KASPERSKY LAB 127
INFORMATIONEN ZU VERWENDETEN FREMDEN CODES 128
Programmcode 128
BOOST 1.30 128
EXPAT 1.2 128
GECKO SDK 1.8 128
INFO-ZIP 5.51 137
LIBNKFM 2.0.5 138
LZMA SDK 4.43 138
OPENSSL 0.9.8D 138
PCRE 7.4 140
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 141
ZLIB 1.2 141
Entwicklungsmittel 141
AUTOCONF 2.61 141
AUTOMAKE 1.10 141
AWK 3.1.5 141
BASH 3.2.33 142
GCC 4.1.2 142
GCC 3.4.5 142
GCC 3.3.6 142
GCC 3.3.2 142
GNU MAKE 3.81 143
GREP 2.5.1 143
PERL 5.8.8 143
SED 4.1.5 145
Sonstige Informationen 145
GNU GENERAL PUBLIC LICENSE 145
SACHREGISTER 167

ÜBER DIESES HANDBUCH

Die Spezialisten von Kaspersky Lab begrüßen Sie herzlich. Wir hoffen, dass die in diesem Handbuch aufgeführten Informationen Ihnen bei Ihrer Arbeit mit Kaspersky Anti-Virus für Lotus Domino behilflich sein werden.

Informationen zur Installation von Kaspersky Anti-Virus sind in diesem Einführungshandbuch angeführt.

Das Handbuch ist für Administratoren von Unternehmensnetzen erstellt worden. Es enthält folgende Informationen: Wie man das Programm einsetzt, Einstellungen anpasst, den Schutz eines Servers sowie einer Server-Gruppe via Domino-Client, Programm-Web-Oberfläche und die Domino-Server-Konsole managen kann.

Falls Sie keine Antwort auf Ihre Frage zu Kaspersky Anti-Virus gefunden haben, können Sie weitere Informationsquellen über Anti-Virus hinzuziehen.

IN DIESEM ABSCHNITT

In diesem Dokument 12

Kennzeichnungen. 14

IN DIESEM DOKUMENT

Dieses Dokument ist folgendermaßen unterteilt:

- *Text des Lizenzvertrages* (s. S. 3). Im diesem Abschnitt ist der Text des Lizenzvertrags zwischen Kaspersky Lab ZAO und dem Endbenutzer aufgeführt. In diesem werden die Rechte und Einschränkungen für die Anwendung Kaspersky Anti-Virus für Lotus Domino bekannt gegeben.

- *Zusätzliche Informationsquellen über das Programm* (s. S. 15). In diesem Abschnitt werden Informationen dargelegt, woher Sie, außer aus den vorliegenden Unterlagen,, weitere Informationen über das Programm erhalten können und falls nötig, wie Sie "Kaspersky Lab"kontaktieren können.

- *Kaspersky Anti-Virus 8.0 für Lotus Domino* (s. S. 17). In diesem Abschnitt sind die neuen Hauptfunktionen von Kaspersky Anti-Virus 8.0 für Lotus Domino beschrieben, bzw. die Unterschiede zur Vorgängerversion dargestellt, sowie die minimalen Hard- und Softwarevoraussetzungen erläutert, welche für die Installation und Ausführung von Kaspersky Anti-Virus nötig sind.

- *Programm-Architektur* (s. S. 21). In diesem Abschnitt wird die Funktionsweise des Programms beschrieben , sowie Informationen zur Einstellungsverwaltung von Kaspersky Anti-Virus und Verwaltung von Benutzerberechtigungen angewiesen.

- Lizenzverwaltung (s. S. 34). In diesem Abschnitt werden sie ausführlich über die Schwerpunkte der Lizenzierung von Kaspersky Anti-Virus informiert., z.B auch , wie eine Lizenz für Kaspersky Anti-Virus installiert oder gelöscht wird.

- *Programmoberfläche* (s. S. 38). Dieser Abschnitt beschreibt die Hauptelemente der Programm-Oberfläche bei der Arbeit mit dem Lotus Notes Client im Web-Browser-Modus.

- *Programm starten und beenden* (s. S. 46). Dieser Abschnitt beschreibt, wie Kaspersky Anti-Virus auf dem Server gestartet und gestoppt wird und wie man sich für die Anpassung der Programmeinstellungen zum Server verbinden kann.

- *Serverschutzzustand* (s. S. 47). Dieser Abschnitt zeigt Ihnen, wie Sie Information über den Anti-Virus Serverschutz einsehen können: Welche Schutzkomponenten aktiviert oder deaktiviert sind oder wie die Komponenten des Anti-Virus Serverschutzes aktiviert und deaktiviert werden.

- *Standardmäßiger Serverschutz* (s. S. 49). In diesem Abschnitt wird beschrieben, wie Kaspersky Anti-Virus mit den standardmäßigen Einstellungen arbeitet.

- *Update der Datenbanken* (s. S. 51). Dieser Abschnitt beschreibt, wie die Update-Einstellungen für Server und Server-Gruppen angepasst werden.Unter anderem, welche Update-Quellen man verwenden kann, wie die Updates der Datenbanken manuell und planmäßig gestartet werden. Außerdem wird das Vorgehen zum von Kaspersky Anti-Virus bei der Installation auf einem bzw.mehreren Servern beschrieben.

- *E-mail-schutz* (s. S. 59). In diesem Abschnitt erfahren Sie, wie der Mail-Schutz für Domino-Server aktiviert und deaktiviert wird, wie man E-Mail-Objekte zur Untersuchung auswählt, wie die Filterung von Anhängen eingestellt wird, wie die Objekt-Verarbeitung der E-Mails nach den Ergebnissen der Anti-Viren-Untersuchung eingestellt wird und wie Benachrichtigungen über Epidemien eingestellt werden.

- *Replikationsschutz* (s. S. 71). Dieser Abschnitt informiert Sie darüber, wie der Replikationsschutz aktiviert oder deaktiviert wird, wie die Replikationsobjekte zur Untersuchung ausgewählt werden, wie die Filterung von Anhängen eingestellt wird, und wie die Verarbeitung der Replikationsobjekte nach Ergebnissen der Anti-.Viren-Untersuchung eingestellt wird.

- *Untersuchung von Datenbanken* (s. S. 78). In diesem Abschnitt werden Sie darüber informiert, wie die Untersuchung von Datenbanken gestartet und gestoppt wird, wie Datenbankobjekte zur Anti-Viren-Untersuchung ausgewählt werden, wie die Filterung von Anhängen eingestellt wird, wie die Verarbeitung von Datenbankobjekten nach einer Anti-Viren-Untersuchung eingestellt wird und wie die Untersuchungseinstellungen angepasst werden.

- *Leistung* (s. S. 89). In diesem Abschnitt sind die Einstellungen beschrieben, welche die Performance bestimmen.

- *Quarantäne* (s. S. 91). In diesem Abschnitt wird erklärt, wie man Objekte, die in die Quarantäne verschoben wurden, einsehen kann, wie deren Verarbeitung eingestellt wird und die Einstellungen der Quarantäne angepasst werden.

- *Ereignisprotokoll und Statistik* (s. S. 98). In diesem Abschnitt erfahren Sie, wie die Einstellungen des Ereignisprotokolls und der Statistik angepasst werden und wie Sie die Ereignisprotokolle und Statistik Datenbank (Information für einen Server oder allgemeine Information über alle Server) einsehen können.

- *Benachrichtigungen* (s. S. 109). In diesem Abschnitt wird beschrieben, wie die Benachrichtigungseinstellungen über die während der Untersuchung entdeckten Objekte angepasst werden.

- *Konfigurationsverwaltung* (s. S. 112). In diesem Abschnitt wird erklärt, wie Profile hinzugefügt oder gelöscht werden, wie ein Server zu einem anderen Profil verschoben wird und wie die Servereinstellungen angepasst werden.

- *Überprüfung der Programmeinstellungen auf richtigkeit* (s. S. 119). In diesem Abschnitt wird beschrieben, wie die Richtigkeit der Programmeinstellungen für jede Schutzkomponente mittels Test-Virus eicar und seiner Modifikationen nachgeprüft wird.

- *Server-Konsolen-Modus* (s. S. 122). In diesem Abschnitt werden die Verwaltungsbefehle aufgelistet, mittels welcher Kaspersky Anti-Virus via Befehlszeile aus der Domino-Server-Konsole verwaltet werden kann.

- *Anfrage an den Technischen Support* (s. S. 124). In diesem Abschnitt sind die Regeln für Anfragen an den technischen Support beschrieben.

- *Glossar* (s. S. 125). In diesem Abschnitt werden die in diesem Handbuch verwendeten Fachbegriffe aufgezählt.

- *Kaspersky Lab* (s. S. 127). In diesem Abschnitt werden Informationen über Kaspersky Lab aufgeführt.

- *Informationen über die Verwendung von Programmcodes von Drittherstellern* (s. S. 128). Im diesem Abschnitt werden Informationen über die im Programm verwendeten Codes von Drittherstellern aufgeführt.

KENNZEICHNUNGEN

In diesem Handbuch werden die in der nachstehend angeführten Tabelle ausgewiesenen Kennzeichnungen verwendet.

Tabelle 1. Kennzeichnungen.

INFORMATIONSTYP	KENNZEICHNUNG
Beachten Sie, dass...	Warnungstext.
Es wird empfohlen … zu verwenden...	Erläuterungstext.
Beispiel: ...	Beispielstext.
CTRL+SHIFT	Namen der Tastaturtasten.
Einschließen	Namen der Oberflächenelemente.
Update	Neuer Begriff.
Um den Aufgabenzeitplan anzupassen, handeln Sie folgenderweise:	Handbuchtext.
`help`	Text eines Systembefehls.

ZUSÄTZLICHE INFORMATIONSQUELLEN ÜBER DAS PROGRAMM

Falls bei Ihnen Fragen, die mit der Auswahl, dem Kauf, der Installation und Verwendung von Kaspersky Anti-Virus 8.0 entstehen, können Sie Antworten auf diese aus verschiedenen Informationsquellen erhalten. Abhängig von der Dringlichkeit und Wichtigkeit Ihrer Frage können Sie eine für Sie geeignete Quelle auswählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche 15

Anfrage an die Vertriebsabteilung 16

Anfrage an die Dokumentationsentwicklungsgruppe 16

Beurteilung von Kaspersky Lab Programmen im Webforum 16

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Sollten bei Ihnen Fragen entstehen, stehen Ihnen folgende Informationsquellen über das Programm zur Verfügung:

- Programm-Seite auf der Webseite von Kaspersky Lab;
- Programm-Seite auf der Webseite des Technischen Supports (in der Wissensdatenbank);
- Elektronisches Hilfesystem;
- Unterlagen.

Seite auf der Webseite von Kaspersky Lab

http://www.kaspersky.com/de/anti-virus_lotus_notes_domino

Auf dieser Seite finden Sie allgemeine Informationen über Kaspersky Anti-Virus, seine Funktionen und Besonderheiten In unserem Online-Shop können Sie Kaspersky Anti-Virus kaufen oder die Nutzungsdauer verlängern.

Seite auf der Webseite des technischen Supports (Wissensdatenbank)

http://support.kaspersky.com/lotus

Auf dieser Seite finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel enthalten nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen (FAQ) zu Kauf, Installation und Anwendung von Kaspersky Anti-Virus. Sie sind nach Themen wie z. B. "Arbeit mit Schlüsseln", "Update der Datenbanken" oder "Beheben von Störungen bei der Arbeit" angeordnet. Die Artikel können auch Fragen behandeln, die nicht nur Kaspersky Anti-Virus sondern auch andere Produkte von Kaspersky Lab betreffen.

Elektronisches Hilfesystem

Die Hilfe enthält Informationen darüber, wie der Serverschutz verwaltet wird: Anzeige des Schutzstatus, Schutzparameter-Einstellung, Aktivieren und Deaktivieren von Schutzkomponenten, Untersuchung von Server-Datenbanken und Update von Anti-Viren-Datenbanken manuell zu starten.

Um die Hilfe zu öffnen, wählen Sie den **Hilfe** Tab im Datenbank-Fenster des Verwaltungscenters.

Unterlagen

Der Unterlagensatz zu Kaspersky Anti-Virus enthält die meisten für seine Anwendung erforderlichen Informationen. Er besteht aus folgenden Dokumenten:

- **Das Administrator-Handbuch** enthält folgende Informationen: Wie man das Programm handhabt, seine Einstellungen anpasst, den Schutz eines Servers sowie auch einer Server-Gruppe via eines Domino-Clients verwaltet und die Programm-Web-Oberfläche über eine Domino-Server-Konsole verwaltet werden kann.

- **Das Implementierungshandbuch** ermöglicht es dem Administrator, das Programm im Netzwerk auszubringen, enthält praktische Empfehlungen zu Programminstallation und Anpassung sowie zur Deinstallation auf einem oder auf allen geschützten Servern im Netzwerk.

ANFRAGE AN DIE VERTRIEBSABTEILUNG

Sollten Fragen zu Auswahl, Kauf oder der Verlängerung der Nutzungsdauer von Kaspersky Anti-Virus entstehen, können Sie sich an die Mitarbeiter der Vertriebsabteilung in unserer Zentrale in Moskau unter folgenden Telefonnummern wenden:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Die Beratung kann auf Englisch sowie Russisch erfolgen.

Sie können auch Ihre Frage an Mitarbeiter der Vertriebsabteilung unter folgender E-Mail-Adresse stellen: sales@kaspersky.com.

ANFRAGE AN DIE DOKUMENTATIONSENTWICKLUNGSGRUPPE

Sollten Sie Fragen zur Dokumentation haben, z.B: falls Sie Fehler gefunden haben oder uns Ihre Meinung zu den Unterlagen mitteilen möchten, wenden Sie sich bitte direkt an unser Redaktionsteam für technische Dokumentation.

Senden Sie uns eine E-Mail mit Ihren Verweisen und Fragen an folgende E-Mail-Adresse: docfeedback@kaspersky.com. Als Betreff geben Sie „Kaspersky Help Feedback: Kaspersky Anti-Virus 8.0 für Lotus Domino" an.

BEURTEILUNG VON KASPERSKY LAB PROGRAMMEN IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Benutzern in unserem Forum unter der folgenden Adresse diskutieren: http://forum.kaspersky.com/index.php?showforum=28.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Kommentare hinterlassen und die Suchfunktion nutzen.

KASPERSKY ANTI-VIRUS 8.0 FÜR LOTUS DOMINO

Kaspersky Anti-Virus 8.0 für Lotus Domino (im Weiteren Kaspersky Anti-Virus) ist für den komplexen Anti-Viren-Schutz von Domino-Servern bestimmt. Das Programm sichert den Schutz des E-Mail-Verkehrs, bietet Replikationsschutz und die Untersuchung der Datenbanken, welche auf dem geschützten Server gespeichert werden.

Kaspersky Anti-Virus wird auf Servern installiert, welche unter den Betriebssystemen Microsoft Windows und Linux laufen und erfüllt folgende Funktionen:

- Untersuchung von allen auf Domino-Server eingehenden, ausgehenden und gerouteten E-Mails. Dabei werden E-Mailtexte, Anhänge und eingebettete OLE-Objekte überprüft. Kaspersky Anti-Virus entdeckt Schädlinge in eingebetteten Archiven und gepackten exe-Dateien, außer in Archiven, welche durch ein Kennwort geschützt sind.

- Untersuchung von Dokumenten, welche nach der Replikation geändert wurden. Die durch eine Replikation geänderten Dokumente werden auf vorhandene Bedrohungen untersucht. Ausgehende Replikationen werden nicht untersucht. Untersucht werden Inhalte von Feldern in RTF-Dokumenten, Anhänge und in Dokumente eingebettete OLE-Objekte.

- Die Untersuchung der Datenbanken des geschützten Servers wird planmäßig oder auf Anforderung durchgeführt. Untersucht werden Inhalte von Feldern in RTF-Dokumenten, Anhänge und in Dokumente eingebettete OLE-Objekte.

- Filterung von Objekten nach Größe und Dateimaskenname bei der Untersuchung von E-Mails, Replikationen und Datenbanken. Gefilterte Objekte werden nach den vom Administrator angegeben Regeln behandelt.

- Verarbeitung von infizierten, möglicherweise infizierten und verdächtigen Objekten, die bei der Untersuchung der E-Mails, der Replikationsdokumente und der Dokumente der Datenbanken entdeckt wurden. Je nach den vorgenommenen Schutz-, bzw. Scaneinstellungen, desinfiziert, löscht oder überspringt Kaspersky Anti-Virus das Objekt, meldet den Administratoren die entdeckte Bedrohung und die Ergebnisse der Objektverarbeitung und speichert statistische Information.

- Sender, Empfänger und Administratoren werden von den in E-Mails entdeckten infizierten, möglicherweise infizierten und verdächtigen Objekten und den ausgeführten Aktionen benachrichtigt.

- Kaspersky Anti-Virus benachrichtigt bei auftretender Gefahr von einer möglichen Epidemie. Kaspersky Anti-Virus registriert jegliche Versuche eines Massenmailings von infizierten, möglicherweise infizierten und beschädigten Objekten in den E-Mails und meldet es den Administratoren.

- Benachrichtigung der Administratoren bei Fund von Objekten, welche bei der Untersuchung von Replikations- und Datenbankendokumenten entdeckt wurden und den ausgeführten Aktionen.

- Speichern von infizierten und möglicherweise infizierten Objekten in der Quarantäne-Datenbank. Dabei werden gespeicherte E-Mails und Dokumente, die bei der Überprüfung der Replikationen sowie bei der Überprüfung der Datenbanken entdeckt wurden, nach Typen gruppiert (E-Mail / Replikationen / Abtastung).

- Speichern der Informationen übern entdeckte infizierte, möglicherweise infizierte und verdächtige Objekte und die jeweils ausgeführten Aktionen in der Ereignisprotokoll- und Statistik Datenbank. Diese werden in einer Textdatei gespeichert sowie zur Informationsdarstellung zur Domino-Server-Konsole weitergegeben.

- Automatisches und manuelles Update der Anti-Viren-Datenbanken via Internet. Als Datenbanken-Update-Ressource können FTP- und HTTP-Update-Server von Kaspersky Lab im Internet, den Updatesatz enthaltende FTP- und HTTP-Server, sowie Netzwerkordner dienen.

Bedrohungserkennung und Behandlung von infizierten Objekten werden anhand der Einträge der Anti-Viren-Datenbanken vollgezogen. Anti-Viren-Datenbanken enthalten Beschreibungen aller bekannten Bedrohungen und Behandlungsweisen für die von ihnen beschädigten Objekten sowie die Beschreibungen für potentiell bösartiger Software.

Es ist höchst wichtig, die Anti-Viren-Datenbanken aktuell zu erhalten, denn neue Bedrohungen entstehen jeden Tag.

Auf den Kaspersky-Lab-Servern werden die Anti-Viren-Datenbanken stündlich aktualisiert. Unsere Empfehlung wäre, die Anti-Viren-Datenbanken genauso oft aktualisieren zu lassen.

- Die Verwaltung von Kaspersky Anti-Virus auf mehreren Servern durch Profile.
- Zugriffsbeschränkung zur Einstellungsanpassung und Betriebsverwaltung von Kaspersky Anti-Virus auf der Server- sowie Profilstufe.
- Einstellungsanpassung und Betriebsverwaltung von Kaspersky Anti-Virus via Lotus Notes Client, Domino-Server-Konsole und Web-Browser.
- Das Programm kann durch den Lotus Notes Client und via Web-Browser installiert und entfernt werden.

IN DIESEM ABSCHNITT

Was gibt es Neues 18

Lieferumfang 19

Service für registrierte Benutzer 19

Hard- und Softwarevoraussetzungen 19

WAS GIBT ES NEUES

Unterschiede von Kaspersky Anti-Virus zur Vorgängerversion bestehen im Folgenden:

- Die Verfahren zur Entdeckung von Bedrohungen wurden mittels des Einsatzes eines neuen Anti-Viren-Kerns weiterentwickelt und verbessert.
- Die Reihe der unterstützten Plattformen wurde erweitert.
- Eine benutzerfreundliche Oberfläche.
- Es wurde eine Option implementiert, die es Ihnen ermöglicht, das Programm durch einen Lotus Notes Client oder über den Web-Browser verwalten zu können.
- Der Befehlssatz zur Verwaltung von Kaspersky Anti-Virus über die Domino-Server-Konsolen wurde erweitert.
- Es wurde eine Option hinzugefügt, das Programm durch einen Lotus Notes Client oder über den Web-Browser zu installieren.
- Es wurde eine Option der Gruppeneinstellung von Parametern und der zentralisierten Verwaltung vom Programm, das auf mehreren Servern installiert ist, durch Profile realisiert.
- Ein verteiltes Schema zur Verwaltung der Sicherheitsparameter der geschützten Server wird unterstützt.
- Ein verteiltes Schema der Ereignisprotokollführung und der Speicherung von Statistiken auf allen geschützten Servern wird unterstützt.

- Die Verwaltung von Benutzerberechtigungen auf Datenbank- oder Dokumentstufe wurde implementiert.
- Die Objektüberprüfung kann im Arbeitsspeicher des Servers stattfinden, ohne dass diese auf die Festplatte gespeichert werden.
- In den E-Mail-Betreff können Informationen über die Überprüfung durch Kaspersky Anti-Virus Überprüfung hinzugefügt werden. Die Information wird nach dem vom Administrator vorgegebenen Muster hinzugefügt.

LIEFERUMFANG

Sie können Kaspersky Anti-Virus bei unseren Vertriebspartnern (CD-Box) sowie im Online-Shop kaufen (zum Beispiel http://www.kaspersky.de, Bereich **Online-Shop**).

Beim Kauf von Kaspersky Anti-Virus im Online-Shop laden Sie das Programm sowie das dazu gehörige Handbuch von der Kaspersky Lab Webseite herunter. Der Aktivierungskode wird Ihnen per E-Mail nach Eingang des Rechnungsbetrages zugestellt.

SERVICE FÜR REGISTRIERTE BENUTZER

Kaspersky Lab bietet den Benutzern ein umfangreiches Spektrum an Leistungen an, die den wirkungsvollen Einsatz des Programms effektiver gestalten.

Beim Lizenzerwerbe werden Sie ein registrierter Benutzer und während der Lizenzlaufzeit können Sie folgende Leistungen nutzen:

- Stündliches Update der Anti-Viren-Datenbanken neuere Versionen dieses Programms;
- Beratung bei Fragen zur Installation, Einstellung und Nutzung des Programms per Telefon und E-Mail;
- Benachrichtigung bei Herausgabe neuer Kaspersky-Lab-Programmen und bei weltweit neu aufgetretenen Viren. Dieser Service wird Benutzern angeboten, die den Newsletter von Kaspersky Lab auf der Webseite des technischen Supports (http://support.kaspersky.com/de/subscribe) abonniert haben.

Es werden allerdings keine Fragen zu Funktion und Gebrauch von Betriebssystemen, zu Software von Dritten sowie zu verschiedenen nicht Kaspersky eigenen Technologien beantwortet.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Damit Kaspersky Anti-Virus optimal funktioniert, muss der Computer folgenden minimalen Voraussetzungen genügen.

Hardware-Voraussetzungen:

- Intel Pentium 32 Bit / 64 Bit oder höher (oder gleichartig).
- 512 MB Arbeitsspeicher (empfohlen wird 1 GB und höher).
- Mindestens ein GB freier Festplattenplatz (empfohlen werden 3 GB und höher).
- Eine empfohlene Größe der Auslagerungsdatei nicht weniger als das zweifache des physikalisch vorhandenen Speichers.

Softwarevoraussetzungen:

Unterstützte Betriebssysteme:

32-Bit Plattformen:

- Microsoft Windows 2000 Server (Service Pack 4 oder höher).
- Microsoft Windows 2000 Advanced Server (Service Pack 4 oder höher).
- Microsoft Windows Server 2003 Standard Edition (Service Pack 2).
- Microsoft Windows Server 2003 Enterprise Edition (Service Pack 2).
- Novell SuSE Linux Enterprise Server 10 (Service Pack 2).
- Red Hat Enterprise Linux 5 (Service Pack 3).

64-Bit Plattformen:

- Microsoft Windows Server 2003 x64 Edition (Service Pack 2).
- Novell SuSE Linux Enterprise Server 10 (Service Pack 2).
- Red Hat Enterprise Linux 5 (Service Pack 3).

Unterstützte Lotus Notes/Domino Server:

- Lotus Notes/Domino Version 6.5
- Lotus Notes/Domino Version 7.0
- Lotus Notes/Domino Version 8.0
- Lotus Notes/Domino Version 8.5

Unterstützte Browser:

- Windows Internet Explorer 7
- Windows Internet Explorer 8
- Mozilla Firefox 3.6
- Google Chrome

PROGRAMM-ARCHITEKTUR

Kaspersky Anti-Virus besteht aus folgenden Modulen:

- **Steuermodul** – bietet folgende Funktionen für Kaspersky Anti-Virus:
  - Programmverwaltung: Initialisiert Untersuchungen von E-Mails und Replikationen, startet Datenbank-Untersuchungen und planmäßige Updates der Anti-Viren-Datenbanken;
  - Einstellungsverwaltung: übernimmt und setzt neue Einstellungen;
  - Speichern und Analyse statistischer Informationen: Schreibt statistische Informationen und Information über Programmereignisse in das Ereignisprotokoll- und Statistikdatenbank und sendet Benachrichtigungen an Administratoren;
  - Benachrichtigung: Sendet E-Mail-Benachrichtigungen über die bei der Untersuchung entdeckten infizierten, möglicherweise infizierten und beschädigten Objekte;
  - Benachrichtigung zu Epidemien: Registriert die Anzahl der während der Untersuchung entdeckten infizierten, möglicherweise infizierten und beschädigten Objekte und die Anzahl der Objekte, die identische Bedrohungen enthalten, und benachrichtigt die Administratoren, falls innerhalb der Vorgabezeit mehr als die voreingestellte Höchstzahl Objekte festgestellt wird;
  - Lizenzverwaltung: Lizenz-Aktivierung, Analyse der Lizenzinformationen, Installation und entfernendes Aktivierungscodes.
- **Modul für die E-Mail- und Replikationsuntersuchung** – führt die Anti-Viren-Prüfung der E-Mails und Replikationen aus.
- **Modul für die Datenbanken-Untersuchung** – führt die Anti-Viren-Prüfung der Domino-Server-Datenbanken aus.

Alle Module werden beim Domino-Server-Start automatisch geladen. Informationen über den Modulbetrieb können in die Ereignisprotokoll und Statistik Datenbank oder in eine Log-Datei von Anti-Virus eingetragen werden und in der Domino-Server-Konsole dargestellt werden.

Alle Datenbanken werden im Ordner der Kaspersky Anti-Virus Datenbanken aufbewahrt (standardmäßig ist das der Ordner kavdatabases).

Das Programm besteht aus folgenden Datenbanken:

- Verwaltungscenter Datenbank (kavcontrolcenter.nsf.) – wird für Verwaltung von Kaspersky Anti-Virus Einstellungen und deren Speicherung verwendet (s. Abschnitt "Kaspersky Anti-Virus Einstellungsverwaltung" auf der S. 26);
- Quarantäne-Datenbank (kavquarantine.nsf) – wird für die Aufbewahrung der in die Quarantäne verschobenen Objekte und deren Verarbeitung verwendet (s. S. 91);
- Ereignisprotokoll und Statistik Datenbank (kaveventslog.nsf) – wird für die Aufbewahrung der im Betrieb von Kaspersky Anti-Virus aufgetauchten Ereignisse sowie der statistischen Informationen über die Ergebnisse der Objektuntersuchung und den ausgeführten Aktionen verwendet (s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98);
- Datenbank Hilfe (kavhelp.nsf) – enthält Hilfeinformationen zur Arbeit mit Kaspersky Anti-Virus.

Der Zugriff zu den aufgezählten Datenbanken ist durch die Benutzeroberfläche der Verwaltungscenter-Datenbank implementiert (s. Abschnitt "Programmoberfläche" auf der S. 38).

IN DIESEM ABSCHNITT

Schema des Anti-Viren-Serverschutzes 22

Kaspersky Anti-Virus Einstellungsverwaltung 26

Einstellungsverwaltung der Konfigurationsdatei notes.ini 28

Berechtigungsverwaltung 30

SCHEMA DES ANTI-VIREN-SERVERSCHUTZES

Der Serverschutz besteht aus folgenden Komponenten: E-Mail-Schutz, Replikationsschutz und Untersuchung der Datenbanken.

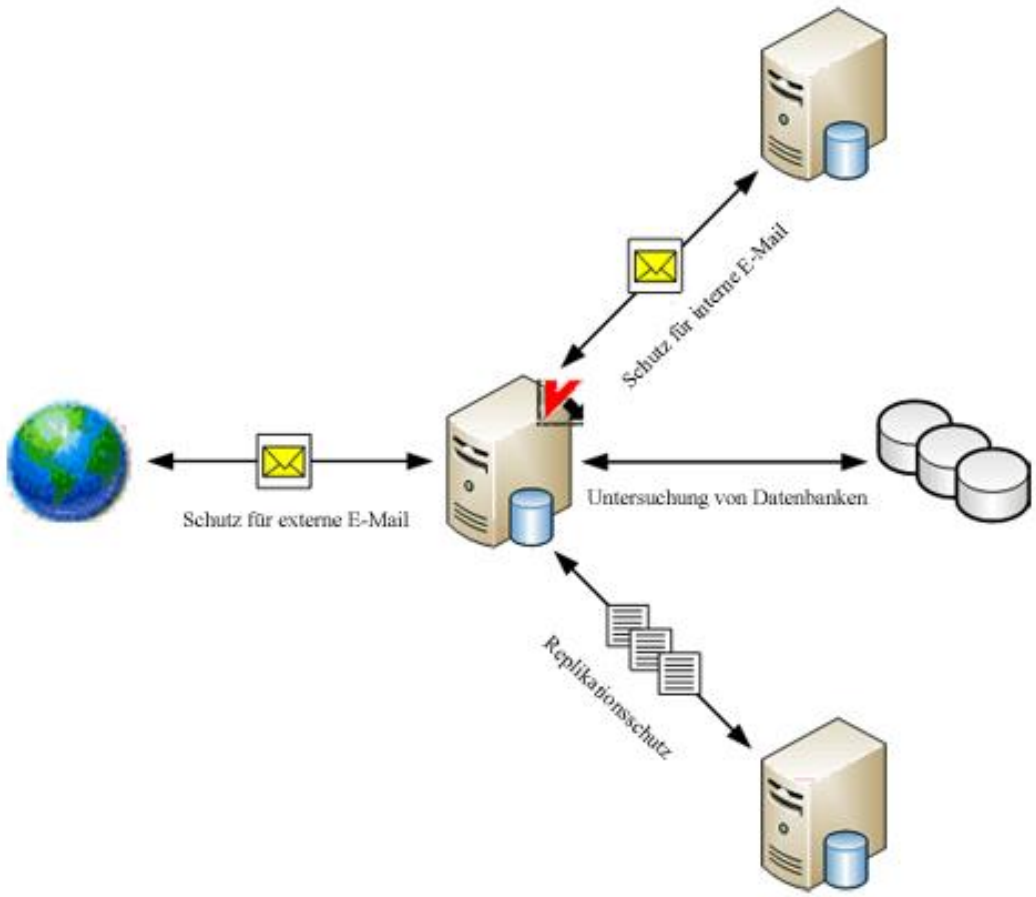


Abbildung 1: Schema des Domino-Server Anti-Viren-Schutzes

IN DIESEM ABSCHNITT

Schema des Programmablaufs 23

Anti-Viren-PrüfAlgorithmus 24

Algorithmus zur Filterung von Anhängen 24

Verarbeitung der Objekte und AUF sie ANGEWANDTE Aktionen 25

SCHEMA DES PROGRAMMABLAUFS

Es ist folgendes Schema des Programmablaufs vorgesehen:

1. Das **Steuermodul** erhält Informationen des geschützten Domino-Servers über in die Mail Box Dienstdatenbank eingehenden E-Mails oder über den Versuch eine Replikation auf dem geschützten Server auszuführen. Das **Steuermodul** gibt die E-Mails oder das infolge der Replikation geänderte Dokument an das **Modul zur E-Mail- und Replikationsuntersuchung**.

2. Das **Modul zur E-Mail- und Replikationsuntersuchung** überprüft die E-Mails / das Dokument und verarbeitet es nach den Einstellungen des E-Mail- und Replikationsschutzes. Dabei werden folgende Aktionen ausgeführt:

   - Untersuchte Objekte werden hervorgehoben. Die E-Mails werden in Meldungskörper, Anhänge und OLE-Objekte aufgeteilt. Im Dokument werden Felder im Rich Text-Format, Anhänge und OLE-Objekte hervorgehoben.

   - Anhänge werden nach Größe, bzw. nach deren Namengefiltert (s. Abschnitt "Algorithmus zur Filterung von Anhängen" auf der S. 24).

   - Objekte werden einer Anti-Viren-Untersuchung unterzogen (s. Abschnitt "Anti-Viren-Prüfalgorithmus" auf der S. 24).

   - Nicht infizierte Objekte werden nicht verändert, die übrigen werden den Schutzeinstellungen entsprechend verarbeitet (s.Abschnitt "Verarbeitung der Objekte und auf sie angewandte Aktionen" auf der S. 25). Vor der Verarbeitung kann eine Objektkopie in der Quarantäne Datenbank gespeichert werden.

   - Verarbeitete E-Mails werden an das E-Mail-System des Domino-Servers zum Versand weitergegeben. Verarbeitete Dokumente werden in den Datenbanken gespeichert.

3. Nach der Anpassung der Benachrichtigungseinstellungen für Epidemien, summiert das die Menge der infizierten, möglicherweise infizierten und beschädigten Objekte, die bei der Untersuchung von E-Mails entdeckt wurden, sowie die Menge der Objekten, die gleichartige Bedrohungen enthalten (s. Abschnitt "Benachrichtigungen über Epidemien" auf der S. 68).

4. Nach dem geplanten Start der Datenbankuntersuchung oder dem manuell eingegebenen Befehl zum Untersuchungsstart übermittelt das **Steuermodul** dem **Modul zur Datenbankuntersuchung** den Befehl, die Untersuchung starten zu lassen. Das **Modul zur Datenbankuntersuchung** erstellt eine Liste der zu Untersuchung ausgewählten Objekte, entsprechend der Untersuchungseinstellungen. Danach werden diese Dokumente anhand dieser Liste untersucht. Der Algorithmus zur Dokumentuntersuchung ist identisch zu dem Algorithmus des **Moduls zur E-Mail- und Replikationsuntersuchung**.

ANTI-VIREN-PRÜFALGORITHMUS

Die Analyse des zur Untersuchung ausgewählten Objekts wird von Kaspersky Anti-Virus nach folgendem Algorithmus ausgeführt:

1. Die Objektuntersuchung wird anhand der Anti-Viren-Datenbank-Einträge ausgeführt. Kaspersky Anti-Virus vergleicht das Objekt mit den Datenbanken-Einträgen, und bestimmt, ob das Objekt ein Schädling ist, zu welcher Klasse der bösartigen Programme es gehört und welche Behandlungsweisen dazu verwendet werden können.

   Anti-Viren-Datenbanken enthalten die Beschreibung und Behandlungsweisen aller zum Zeitpunkt der Anti-Viren-Datenbanken-Entstehung bekannten bösartigen Programme, Scherz-Programme, potentiell gefährlichen Programme, sowie Programme, die nicht potentiell gefährlich sind, doch Teil einer Software zu deren Entwicklung sein können.

   Bei der Objektüberprüfung wird eine inkrementelle Untersuchung verwendet. Die Dateien werden nur nach einer Änderung erneut untersucht, d. h., falls das Datum der letzten Datei-Änderung älter als das Datum der letzten Untersuchung ist, wird die Datei nicht überprüft. Man kann die inkrementelle Untersuchung deaktivieren, indem man die Variable KAVNonIncrementalScan=1setzt. Standardmäßig ist diese Variable nicht gesetzt.

   Basierend auf den Untersuchungsergebnissen wird dem Objekt einer der folgenden Status zugewiesen:

   - *nicht infiziert* – das Objekt enthält keine Bedrohungen.
   - *nicht desinfizierbar* – das Objekt enthält eine Bedrohung, welche durch den Einsatz der vorhandenen Anti-Viren-Datenbanken-Version nicht entfernt werden kann. Diese Objekte können nicht behandelt werden.
   - *desinfizierbar* – das Objekt enthält eine Bedrohung, welche durch den Einsatz der vorhandenen Anti-Viren-Datenbanken-Version desinfiziert werden kann. Nachdem die Behandlung beendet ist, wird das Objekt als nicht infizierte geführt.
   - *nicht geprüft* – Kaspersky Anti-Virus ist es nicht gelungen, das Objekt zu untersuchen. Eventuell ist das Objekt ein Kennwortgeschütztes oder ein mit einem unbekannten Algorithmus gepacktes Archiv. Eventuell ist bei der Objektuntersuchung ein Fehler aufgetreten oder die Untersuchungsdauer wurde überschritten.

2. Das Objekt, welches den Ergebnissen der Untersuchung nach als nicht infizierte geführt wurde, wird zusätzlich einer heuristischen Analyse unterzogen. Dabei analysiert Kaspersky Anti-Virus die Aktivität des zur Untersuchung ausgewählten Objekts mit speziellen Mechanismen. Falls diese Aktivität typisch für Schädlinge ist, wird das Objekt als *möglicherweise infiziert* geführt: D. h. dass der Objektcode entweder einem modifizierten Code eines bekannten Virus oder einem virenähnlichen Code enthält, welcher bis jetzt noch nicht bekannt und in den Anti-Viren-Datenbanken von Kaspersky Lab nicht beschrieben ist.

ALGORITHMUS ZUR FILTERUNG VON ANHÄNGEN

Kaspersky Anti-Virus filtert in E-Mails und Dokumenten eingebettete Objekte aus. Falls das Objekt den Filterbedingungen entspricht, wird ihm der in den Filtereinstellungen angegebene Status zugewiesen. Es wird keine weitere Anti-Viren-Untersuchung des Objekts ausgeführt. Das Objekt wird nach dem bei der Filterung zugewiesenen Status verarbeitet: Es werden die Aktionen ausgeführt, welche für Objekte dieses Status in den Einstellungen des E-Mail- und Replikationsschutzes sowie den Datenbank-Untersuchungen angegeben wurden (s. Abschnitt "Verarbeitung der Objekte und auf sie angewandte Aktionen" auf der S. 25).

Im Programm sind folgende Typen der Anhangsfilterung vorgesehen:

- **Filterung nach Größe**. Kaspersky Anti-Virus untersucht die Größe von Anhängen. Falls die Objektgröße den maximal zulässigen Wert überschreitet, wird dem Objekt der in den Filtereinstellungen angegebene Status zugewiesen und keine Anti-Viren-Untersuchung wird ausgeführt. Das Objekt, dessen Größe kleiner als der angegebene Wert ist, wird zur Anti-Viren-Untersuchung weitergegeben.

- **Filterung nach Name**. Kaspersky Anti-Virus untersucht die Namen der Anhänge. Falls ein Objektname mit den in den Filtereinstellungen angegebenen Dateimasken übereinstimmt, wird dem Objekt der in den Filtereinstellungen angegebene Status zugewiesen und keine Anti-Viren-Untersuchung wird ausgeführt. Falls der Objektname mit keiner von den in den Filtereinstellungen eingegebenen Dateimasken übereinstimmt, wird es zur Anti-Viren-Untersuchung weitergegeben.

Falls in den Schutzeinstellungen beide Typen der Anhangsfilterung konfiguriert sind, untersucht Kaspersky Anti-Virus zuerst die Objektgröße. Nachdem, falls die Objektgröße kleiner ist, als in den Filtereinstellungen nach Größe eingegebener Wert ist, untersucht Kaspersky Anti-Virus den Objektnamen. Falls Objektgröße größer als in Filtereinstellungen nach Größe eingegebener Wert ist, untersucht Kaspersky Anti-Virus den Objektnamen nicht.

Den Untersuchungsergebnissen entsprechend kann dem Objekt einer der folgenden Status zugewiesen werden:

- nicht infiziert;
- nicht desinfizierbar;
- nicht geprüft;
- möglicherweise infiziert.

Die Einstellungen zur Anhangsfilterung werden in den Einstellungen des E-Mail-Schutzes, des Replikationsschutzes und der Datenbanken-Untersuchung, für jede einzelne Schutzkomponente separat festgelegt.

VERARBEITUNG DER OBJEKTE UND AUF SIE ANGEWANDTE AKTIONEN

Kaspersky Anti-Virus verarbeitet Objekte entsprechend dem Status, der ihnen während der Anti-Viren-Untersuchung zugewiesen wurde (s. Abschnitt "Anti-Viren-Prüfalgorithmus" auf der S. 24) und nach den Ergebnissen der Anhangsfilterung (s. Abschnitt "Algorithmus zur Filterung von Anhängen" auf der S. 24). Nicht infizierte Objekte werden ohne jegliche Änderungen an die Datenbanken (Replikationsschutz und Datenbanken-Untersuchung) oder das E-Mail-System des Domino-Servers (E-Mail-Schutz) weitergegeben. An den übrigen Objekten können folgende Aktionen ausgeführt werden:

- **Desinfizieren**. Kaspersky Anti-Virus führt die Desinfizierung des Objekts anhand der in den Anti-Viren-Datenbanken hinterlegten Informationen über die im Objekt entdeckte Bedrohung aus. Als Ergebnis wird die im Objekt enthaltene Bedrohung desinfiziert. Das Objekt wird als nicht infiziertes geführt und in der Datenbank mit seiner Ursprungsadresse gespeichert oder ans E-Mail-System weitergegeben.

  Unabhängig von den gewählten-Programmeinstellungen erfolgt die Desinfektion von OLE-Objekten immer durch Löschen.

- **Überspringen**. Kaspersky Anti-Virus gibt das Objekt ohne jegliche Änderungen weiter.

- **Löschen**. Kaspersky Anti-Virus löscht das Objekt aus dem Dokument oder aus der E-Mails.

Die Aktionen, welche das Programm ausführen wird, werden für jeden einzelnen Status in den Einstellungen des E-Mail und Replikationsschutzes sowie der Datenbanken-Untersuchung separat angepasst.

Vor der Verarbeitung kann eine Kopie des Objekts in der Quarantäne Datenbank gespeichert werden. Informationen über ausgeführte Aktionen können in der Ereignisprotokoll- und Statistik Datenbank gespeichert werden.

Kaspersky Anti-Virus kann den Administratoren sowie den E-Mailabsendern und Empfängern (E-Mail-Schutz), Meldung überentdeckte Objekte und ausgeführte Aktionen melden (s. Abschnitt "Benachrichtigungen" auf der S. 109).

KASPERSKY ANTI-VIRUS EINSTELLUNGSVERWALTUNG

Die Verwaltung von Kaspersky Anti-Virus wird durch Profilparameter und Serverparameter realisiert.

Das Profil stellt alle Programmeinstellungen für eine Server-Gruppe, die diesem Profil zugehören, zur Verfügung. Durch Profilmechanismus wird integrierte Parameterverwaltung von Kaspersky Anti-Virus ausgeführt.

Das Profil kann sowohl mehrere, als auch nur einen Server einschließen. Im Falle eines isolierten Ausbringungsschemas von Kaspersky Anti-Virus schließt das Profil nur ein Server ein (s. Implementierungshandbuch für Kaspersky Anti-Virus 8.0 für Lotus Domino).

Durch Profile können dazu genutzt werden, sämtliche Einstellungen zu konfigurieren, außer wenn es um die vom Server verwendete Lizenz und der Speicherdauer der in die Quarantäne verschobenen Objekte geht. Diese zwei Einstellungen werden nur für einzelne Server angegeben und in den Servereinstellungen festgelegt (s. Abschnitt "Anpassung der einzelnen ServerEinstellungswerte" auf der S. 115). Außerdem können in den Servereinstellungen einige vom Profil vorgegebene Einstellungen neu gesetzt werden. Dies bietet die Möglichkeit, , Einstellungen für einzelne Server festzulegen, die sich von den im Profil angegebenen Werten unterscheidet. Zu diesen Einstellungen zählen beispielsweise Update-Einstellungen, Einstellungen zur Ereignisaufbewahrung, sowie statistische Informationen.

Server werden bei der Installation von Kaspersky Anti-Virus automatisch zum Profil hinzugefügt. Bei einer Deinstallation wird der Server automatisch aus dem Profil entfernt. Das Profil schließt nur Server ein, welche durch Kaspersky Anti-Virus geschützt sind.

Sie können Profile erstellen und löschen (s. Abschnitt "Profile erstellen und löschen" auf der S. 112). Sie können einen Server, auf welchem Kaspersky Anti-Virus installiert ist, von einem zum anderen Profil verschieben (s. Abschnitt "Server zu einem anderen Profil verschieben" auf der S. 115).

Durch Profile können Sie einheitliche Einstellungen von Kaspersky Anti-Virus für eine Server-Gruppe festlegen, z.B. basierend auf deren geographischen Standort, ausführenden Funktionen oder von anderen Faktoren ausgehend. Diese Option vereinfacht die Programmverwaltung wesentlich, wenn sie auf mehreren Servern installiert wird, und ermöglicht es, den Status des Anti-Viren-Schutzes auf allen Computern zentralisiert zu kontrollieren.

Sie können auch Profile mit verschiedenen Sicherheitsniveaus erstellen und z. B. für E-Mail-Server oder Datenbank-Server verwenden. Dazu können Sie mehrere Profile mit verschiedenen Einstellungen erstellen. Um einem Server oder einer Server-Gruppe ein bestimmtes Sicherheitsniveau zuzuweisen, genügt es, den Server zu dem Profil mit den entsprechenden Einstellungen zu verschieben.

Durch die Servereinstellungen können Sie die Einzelwerte, den Serverfunktionen im Netzwerk entsprechendanpassen (s. Abschnitt "Anpassen der Einzelwerte der Servereinstellungen" auf der S. 115). So, z. B., kann durch die Servereinstellungen ein zentralisiertes Schema der Anti-Viren-Datenbanken-Updates erstellt werden (s. Abschnitt "Update-Schema" auf der S. 53).

Sämtliche Informationen zu den Kaspersky Anti-Virus Einstellungen werden in der Verwaltungscenter Datenbank gespeichert – kavcontrolcenter.nsf. Die Verwaltungscenter Datenbank wird bei der Programminstallation im Ordner der Kaspersky Anti-Virus Datenbank erstellt (standardmäßiger Ordner: kavdatabases). Dabei wird in der Datenbank ein Profil erstellt, zu welchem die geschützten Server hinzugefügt werden. Den Profil- und Serverparametern werden standardmäßige Werte zugewiesen.

Falls ein verteiltes Ausbringungsschemas von Kaspersky Anti-Virus existiert(s. Kaspersky Anti-Virus 8.0 für Lotus Domino Implementierungshandbuch) enthält die kavcontrolcenter.nsf Datenbank Informationen über jede Server, auf welchem das Programm installiert wurde. Die Datenbank wird auf einem dieser Server erstellt, danach wird auf jedem nachfolgenden Server ein Replikat von der vorhandenen Verwaltungscenter Datenbank erstellt. Als Basis wird die Datenbank von einem der Server (je nach Wahl des Administrators), auf dem Kaspersky Anti-Virus bereits installiert ist, verwendet. Der neue geschützte Server wird zu dem Profil hinzugefügt wie der Server, von welchem das Replikat der kavcontrolcenter.nsf. Datenbank erstellt wurde. Den Servereinstellungen werden standardmäßige Werte zugewiesen. Beim Entfernen von Kaspersky Anti-Virus von einem der Server wird die Information über diesen Server aus dem Profil sowie aus der Verwaltungscenter Datenbank gelöscht.

Im Falle eines isolierten Ausbringungsschemas befindet sich die kavcontrolcenter.nsf Datenbank auf einem Server und enthält ausschließlich Konfigurationsinformation für diesen Server.

Zur Einstellungsanpassung und Verwaltung öffnen Sie die kavcontrolcenter.nsf. Datenbank.

Über die benötigten Rechte zum Öffnen der kavcontrolcenter.nsf Datenbank, zur Einstellungsanpassung oder zur Verwaltung von Kaspersky Anti-Virus verfügen nur jene Benutzer, welche die Berechtigungen einer der drei Funktionsgruppen besitzen: **Sicherheitsadministratoren**, **ControlCenter-Administratoren** und **Administratoren mit eingeschränkten Berechtigungen**. Bevor Sie die Datenbank öffnen, überzeugen Sie sich davon, dass das Benutzerkonto die erforderlichen Berechtigungen für die Ausführung der notwendigen Aktionen besitzt (Erstellen, Löschen von Profilen, Profileinstellungsanpassung, Servereinstellungsanpassung usw.).

Die kavcontrolcenter.nsf Datenbank kann auf jedem der geschützten Servern durch einen Lotus Notes Client oder durch einen Web-Browser geöffnet werden (s. Abschnitt "Programmoberfläche" auf der S. 38).

Standardmäßig werden Änderungen von Profil- und Servereinstellungen in das Datenbankreplikat auf dem Server, mit welchem Sie verbunden sind, eingetragen. Beim Replikationsprozess werden Änderungen auf alle anderen geschützten Server verbreitet. Zwischen der Änderung einer Einstellung und ihrer Anwendung kann eine gewisse zeitliche Verzögerung entstehen. Deshalb sollten Sie bei der Auswahl des Servers, auf welchem die Änderungen durchgeführt werden, die Replikationstopologie beachten.

Falls Sie mit Kaspersky Anti-Virus via Lotus Notes Client arbeiten, können Änderungen der Servereinstellungen in das Replikat der Verwaltungscenter Datenbank eingetragen werden, die sich auf dem Server befindet, dessen Parameter Sie bearbeiten. Dies ist unabhängig davon, zu welchem Server Sie verbunden sind (s. Abschnitt "Verwendung der Option der direkten Bearbeitung der Servereinstellungen" auf der S. 118). In diesem Fall werden die neue Werte wesentlich schneller angewandt. Bei der Arbeit über den Web-Browser wird die oben beschriebene Option nicht unterstützt und Änderungen der Serverparameter werden immer in das geöffnete Replikat eingetragen.

Falls im Tab **Allgemeine Einstellungen** im Bereich **Konfiguration verwalten** eines Serverdokuments das Häkchen **Dokument auf dem geschützten Server ändern** gesetzt ist, wird das Dokument aus dem Replikat der Datenbank geöffnet, das sich auf dem Server befindet, der dem Serverdokument entspricht. Im Client der Version 8 und höher wird das Dokument per Mausklick in der Navigationsleiste geöffnet. Bei älteren Clientversionen ist ein Doppelklick nötig. Per Mausklick auf das Dokument in der älteren Client-Version, wird das Dokument aus dem Replikat geöffnet, das sich auf dem aktuellen Server befindet.

Die Arbeit mit der Verwaltungscenter Datenbank kann gleichzeitig an mehreren Arbeitsstationen oder parallel durch Web-Browser und Lotus Notes Client ausgeführt werden. Dabei können gleichzeitige Änderungen von Einstellungen desselben Profils oder Servers durch zwei oder mehrere Benutzern einen Konflikt bei der Replikation verursachen. Außerdem wird es nicht empfohlen, gleichzeitig Änderungen in den Servereinstellungen und in den Einstellungen des Profils vorzunehmen, welches diesen Server einschließt. Nach der Anwendung der neuen Profileinstellungen, können die Servereinstellungen automatisch neu festgelegt werden.

EINSTELLUNGSVERWALTUNG DER KONFIGURATIONSDATEI NOTES.INI

Man kann die Einstellungen von Kaspersky Anti-Virus durch seine Oberfläche oder durch Änderungen in der Konfigurationsdatei notes.ini anpassen.

Um die Einstellungen in der Konfigurationsdatei zu ändern, führen Sie folgende Aktionen aus:

1. Öffnen Sie die Datei mit den Servereinstellungen Domino notes.ini.
2. Passen Sie die Einstellungen an und speichern Sie die Änderungen.
3. Starten Sie den Domino Server neu.

Einstellungen, welche in der Datei notes.ini angegeben sind, werden mit den Einstellungen, die in der Kaspersky Anti-Virus Oberfläche angegeben sind, nicht synchronisiert. Die Einstellungen der Konfigurationsdatei sind höherwertig als die Einstellungen über die Oberfläche.

Tabelle 2. Liste der redigierten Parameter

PARAMETER	WERT	BESCHREIBUNG
EXTMGR_ADDINS	Pfad zu kavmailhook.	Interceptor funktioniert.
	0 / Variablenwert fehlt.	Interceptor funktioniert nicht. ACHTUNG: falls der Variablenwert fehlt, gleicht dies einer Deinstallation von Kaspersky Anti-Virus von diesem Server.
KAVDefaultLogLevel	0	Standard.
	1	Erweitert.
	2	Debugging.
KAVCustomUpdUrlOnly	1	Der Server wird nur über die von Ihnen vorgegebenen Update-Quelle aktualisiert.
	2	Falls es dem Server nicht gelingt, ein Update von der vorgegebenen Quelle auszuführen, versucht Kaspersky Anti-Virus sich mit einer andere Update-Quelle zu verbinden – Dabei wird versucht, sich an die Ressource zu wenden, von welcher das letzte erfolgreiche Update ausgeführt wurde oder an den Kaspersky Lab Update-Server.

PARAMETER	WERT	BESCHREIBUNG
KAVDefaultLogFileName	server - Grundeinstellung.	Name der Log-Datei. Sie können dieser Einstellung einen beliebigen Wert zuweisen. Die Log-Datei wird unter dem Namen, welcher in dieser Angabe vorgegeben wird, erstellt. Die Datei wird sich im Log-Ordner "kavcommon/logs/" befinden. Standardmäßig wird der Dateiname dem folgenden Prinzip nach generiert: <Dateiname>.log_N, wobei N — die Ordnungsnummer der Log-Datei ist. Falls Sie in dieser Einstellung als Dateiname myfile eingeben, so werden die Ereignisse in der Datei myfile.log_N gespeichert.
KAVLogFileSize	2000 KB	Die Größe einer Log-Datei in KB. Um die Schnelligkeit zu optimieren, werden Abweichungen von 5% der vorgegebenen Größe zugelassen.
KAVLogFilesNumber	5	Anzahl der Log-Dateien.
KAVArchDepthLevel	32	Tiefe der Archivverschachtelung.
	0 / Fehlen vom Parameter	Anzahl der Archivverschachtelung ist unbeschränkt.
KAVNonIncrementalScan	0 / Variablewert fehlt	Inkrementelle Untersuchung aktiviert.
	1	Inkrementelle Untersuchung deaktiviert.

BERECHTIGUNGSVERWALTUNG

Die Verwaltung der Benutzerrechte, wird auf ACL Ebene der Kaspersky Anti-Virus Datenbanken sowie auf Ebene einzelner Dokumente (Profil- und Serverparameter) ausgeführt. Berechtigungen auf ACL Ebene werden mit Hilfe der Funktionsgruppen garantiert (s. Abschnitt "Berechtigungsverwaltung auf ACL Ebene der Kaspersky Anti-Virus Datenbanken" auf der S. 30). Berechtigungen auf Dokumentebene werden mit Hilfe von funktionale Rollen gewährt (s. Abschnitt "Berechtigungsverwaltung auf Ebene der Profil- / Servereinstellungen" auf der S. 33).

IN DIESEM ABSCHNITT

Berechtigungsverwaltung auf ACL Ebene der Kaspersky Anti-Virus Datenbanken 30

Berechtigungsverwaltung auf Ebene der Profil- / Serverparameter 33

BERECHTIGUNGSVERWALTUNG AUF ACL EBENE DER KASPERSKY ANTI-VIRUS DATENBANKEN

Für die Gewährung von Berechtigungen auf ACL Ebene der Kaspersky Anti-Virus Datenbanken sind im Programm drei Funktionsgruppen vorgesehen: **Sicherheitsadministratoren**, **ControlCenter-Administratoren** und **Administratoren mit eingeschränkten Berechtigungen**.

Der Bestand jeder Funktionsgruppe wird bei der Programminstallation festgestellt. Der Administrator, der die Installation durchführt, bildet die Funktionsgruppen, indem er Benutzer und / oder Benutzergruppen aus dem Adressbuch des Domino-Servers wählt. Bei der Programminstallation werden die Elemente jeder Funktionsgruppe automatisch in die ACL der Kaspersky Anti-Virus Lotus Notes Datenbanken mit eingeschlossen.

In die ACL der Kaspersky Anti-Virus Datenbanken enthalten auch die Default (Standardmäßig) und Anonymous (Anonym) Einträge und die Server, auf welchen das Programm installiert ist. Server, die in ACL aufgenommen werden sollen, werden vom Administrator bei der Programminstallation angegeben (s. Implementierungshandbuch). Den Servern wird die Zugriffsebene Manager (Verwalter) mit den Rechten, Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten zugewiesen. Für die Einträge Default (Standardmäßig) und Anonymous (Anonym) in die ACL der Kaspersky Anti-Virus Datenbanken wird die Zugriffsebene No access (Kein Zugriff) festgelegt.

BERECHTIGUNGEN DER FUNKTIONSGRUPPEN

Die Berechtigungen der Funktionsgruppen in den ACL Datenbanken von Kaspersky Anti-Virus werden in der Tabelle unten aufgezählt.

Tabelle 3. Berechtigungen der Funktionsgruppen

FUNKTIONSGRUPPEN	DATENBANK VERWALTUNGSCENTER	DATENBANK EREIGNISPROTOKOLL UND STATISTIK	DATENBANK QUARANTÄNE	DATENBANK HILFE
SICHERHEITSADMINISTRATOREN	Zugriffsebene Manager (Verwalter) mit den Rechten auf Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten. Rolle AppAdmin.	Zugriffsebene Manager (Verwalter) mit den Rechten auf Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten.	Zugriffsebene Manager (Verwalter) mit den Rechten auf Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten.	Zugriffsebene Manager (Verwalter).
ADMINISTRATOREN VON VERWALTUNGSCENTER	Zugriffsebene Author (Verfasser) mit den Rechten auf Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten. Rolle AppAdmin.	Zugriffsebene Author (Verfasser) mit den Rechten auf Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten.	Zugriffsebene Author (Verfasser) mit den Rechten auf Erstellung, Löschen von Dokumenten sowie Replikation oder Kopieren von Dokumenten.	Zugriffsebene Reader (Leser).
ADMINISTRATOREN MIT BESCHRÄNKTEN BERECHTIGUNGEN.	Zugriffsebene Author (Verfasser) mit dem Recht auf Replikation oder Kopieren von Dokumenten.	Zugriffsebene Author (Verfasser) mit dem Recht auf Replikation oder Kopieren von Dokumenten.	Zugriffsebene Author (Verfasser) mit dem Recht auf Replikation oder Kopieren von Dokumenten.	Zugriffsebene Reader (Leser).

Nach der Installation von Kaspersky Anti-Virus werden den Benutzern und Benutzergruppen, welche den Funktionsgruppen hinzugefügt wurden, Berechtigungen die für die Arbeit mit dem Programm nötig sind, gewährt.

Benutzer, die in die Gruppe **Sicherheitsadministratoren** eingeschlossen sind, verfügen über maximale Berechtigungen bei der Arbeit mit Kaspersky Anti-Virus und können folgende Aktionen ausführen:

- Berechtigungsverwaltung auf ACL Ebene der Kaspersky Anti-Virus Datenbanken.
- Profile erstellen / löschen.
- Anpassung der Parameter aller Profile und aller Server.
- Löschen der Einträge aus den Quarantäne-, Ereignisprotokoll- und Statistikdatenbanken.

Benutzer, die der Gruppe **ControlCenter-Administratoren** hinzugefügt wurden, können bei der Arbeit mit Kaspersky Anti-Virus folgende Aktionen ausführen:

- Profile erstellen / löschen.

- Anpassung der Parameter aller Profile und aller Server.
- Löschen der Einträge aus den Quarantäne-, Ereignisprotokoll- und Statistikdatenbanken.

Benutzer, die zur Gruppe **Administratoren mit eingeschränkten Berechtigungen** hinzugefügt wurden, verfügen standardmäßig über keine Rechte auf die Anpassung der Einstellungen von Profilen / Servern und das Löschen der Einträge aus den Quarantäne-, Ereignisprotokoll- und Statistikdatenbanken. Die Rechte, welche für die Arbeit mit dem Programm nötig sind, werden den Benutzern dieser Gruppe mit Hilfe der funktionale Rollen gewährt (s. Abschnitt "Berechtigungsverwaltung auf Ebene der Profil- / Serverparameter" auf der S. 33).

Über die Rechte zur Ansicht der der Quarantäne-, Ereignisprotokoll- und Statistikdatenbankeinträge, verfügen die Benutzer aller drei Funktionsgruppen.

GARANTIEREN DER BERECHTIGUNGEN VON FUNKTIONSGRUPPEN FÜR BENUTZER

Bei der Installation von Kaspersky Anti-Virus kann der Administrator einzelne Domino-Benutzer und Benutzergruppen zu jeder der drei Funktionsgruppen hinzufügen.

Zur Vereinfachung des Verfahrens wird empfohlen, nicht einzelne Benutzer sondern Gruppen, die im Adressbuch des Domino-Server gebildet wurden, zu Funktionsgruppen hinzuzufügen (s. Implementierungshandbuch). Bei der Installation werden diese Gruppen zu den ACL Datenbanken von Kaspersky Anti-Virus hinzugefügt. Ihnen werden Berechtigungen der Funktionsgruppen gewährt (s. Abschnitt "Berechtigungen der Funktionsgruppen" auf der S. 31). Weiterhin kann der Administrator des Domino-Servers den Benutzern Berechtigungen gewähren oder sie beschränken, indem er den Gruppenbestand im Adressbuch ändert (Benutzer mit einschließt oder ausschließt).

Falls bei der Programminstallation keine Benutzergruppen sondern nur einzelne Benutzer zu den Funktionsgruppen hinzugefügt wurden, ist es weiterhin erforderlich, die ACL aller Datenbanken von Kaspersky Anti-Virus manuell zu bearbeiten. Um dem Benutzer die Berechtigungen der Funktionsgruppe zu entziehen, muss man sein Benutzerkonto von der ACL aller Datenbanken von Kaspersky Anti-Virus entfernt werden. Um dem Benutzer die Berechtigungen der einen oder anderen Funktionsgruppe zuzuweisen, muss man sein Benutzerkonto in die ACL aller Datenbanken einschließen.

Nur Benutzer, die über Berechtigungen der Funktionsgruppe **Sicherheitsadministratoren** verfügen, können Änderungen in ACL Datenbanken von Kaspersky Anti-Virus vornehmen.

Es wird empfohlen, die Benutzerkonten der ACL Datenbanken von Kaspersky Anti-Virus dieser Gruppe zuzuweisen.

➧ *Um dem Benutzer Berechtigungen der Funktionsgruppe zu gewähren, führen Sie folgende Aktionen aus:*

1. Im Adressbuch des Domino-Servers erstellen Sie eine Gruppe mit einem einzigartigen Namen, beispielsweise, ControlCenterAdmins.
2. Zur Gruppe ControlCenterAdmins fügen Sie den Benutzer hinzu, welchem die Berechtigungen der einen oder anderen Funktionsgruppe, beispielsweise der Gruppe **ControlCenter-Administratoren** gewährt werden sollen.
3. Loggen Sie sich am System mit dem Benutzerkonto ein, welches über die Berechtigungen der Funktionsgruppe **Sicherheitsadministratoren** verfügt.
4. Fügen Sie die Gruppe ControlCenterAdmins zu den ACL Datenbanken von Kaspersky Anti-Virus (Verwaltungscenter, Ereignisprotokoll und Statistik, Quarantäne, Hilfe) hinzu und weisen dieser Berechtigungen zu, die den Berechtigungen der Funktionsgruppe 4. **ControlCenter-Administratoren** entsprechen (s. Abschnitt "**Berechtigungen der Funktionsgruppen**" auf der S. 31).

BERECHTIGUNGSVERWALTUNG AUF EBENE DER PROFIL- / SERVERPARAMETER

Für eine Abgrenzung des Zugriffs auf Ebene einzelner Dokumente (Profil- und Serverparameter) sind folgende funktionale Rollen vorgesehen:

- *Der Administrator des Profils* – verfügt über Rechte zur Ausführung folgender Aktionen:
  - Anpassung der Profileinstellungen und Einstellungen aller Server des Profils.
  - Löschen der Einträge aus den Quarantäne-, Ereignisprotokoll- und Statistikdatenbanken für Server des Profils.
- *Der Administrator des Servers* – verfügt über Rechte zur Ausführung folgender Aktionen:
  - Anpassung der Servereinstellungen, einschließlich Verschieben des Servers in ein anderes Profil.
  - Löschen der Einträge aus den Quarantäne-, Ereignisprotokoll- und Statistikdatenbanken für den Server.

Administratoren von Profilen und Servern werden nach der Programminstallation bestimmt. Die Bestimmung wird für jeden Server (s. Abschnitt "Einsetzung vom Serveradministrator" auf der S. 114) und jedes Profil getrennt ausgeführt (s. Abschnitt "Einsetzung vom Profiladministrator" auf der S. 114).

Als Administrator des Profils und Administrator des Servers kann nur ein Benutzer, der über Berechtigungen einer der drei Funktionsgruppen verfügt, bestimmt werden (s. Abschnitt "Berechtigungsverwaltung auf ACL Ebene der Kaspersky Anti-Virus Datenbanken" auf der S. 30).

Standardmäßig werden die Benutzer und / oder Gruppen in den Profil- und Servereinstellungen als Administratoren angegeben, welche bei der Programminstallation zur Funktionsgruppe **ControlCenter-Administratoren** hinzugefügt wurden.

Unabhängig von der Funktionsrolle wird den Benutzern der Gruppen **Sicherheitsadministratoren** und **ControlCenter-Administratoren** das Recht gewährt, die Einstellungen aller Server und Profile zu bearbeiten. Um eingeschränkte Berechtigungen, beispielsweise, die Anpassung der Einstellungen nur eines Profils / Servers zu zuzuweisen, muss man als Administratoren der Profilen / Servern einen Benutzer aus der Funktionsgruppe **Administratoren mit eingeschränkten Berechtigungen** bestimmen. Den Benutzern dieser Gruppe wird das Recht gewährt, Einstellungen nur von den Profilen / Servern, , zu bearbeiten, für welche sie als Administrator bestimmt wurden. Falls der Benutzer aus dieser Gruppe zum Profiladministrator bestimmt wird, wird ihm auch das Recht gegeben, Einstellungen aller in diesem Profil zugehörenden Server zu bearbeiten.

LIZENZVERWALTUNG

Bezüglich der Lizenzierung von Kaspersky Lab Programmen ist es wichtig sich mit den folgenden Begriffen vertraut zu machen:

- Lizenzvertrag;
- Lizenz;
- Schlüsseldatei.

Diese Begriffe sind untrennbar miteinander verbunden und definieren das Lizenzschema.

Lassen Sie uns diese Begriffe eingehend betrachten.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag 34

Über die Kaspersky Anti-Virus-Lizenzen 35

Über die Kaspersky Anti-Virus-Schlüsseldatei 35

Installation der Schlüsseldatei 36

ÜBER DEN LIZENZVERTRAG

Lizenzvertrag – ist ein Vertrag zwischen einer Einzel- oder Rechtsperson und Kaspersky Lab ZAO, die berechtigt ein Kaspersky Anti-Virus-Exemplar besitzt,. Der Vertrag wird dem Lieferumfang jedes Kaspersky Lab Programms beigelegt. In diesem werden ausführliche Informationen über Rechte und Beschränkungen der Kaspersky Anti-Virus Nutzung angeführt.

In diesem Handbuch können Sie sich mit dem Text des Lizenzvertrags vertraut machen(s. Abschnitt "Text des Lizenzvertrags" auf der S. 3).

Laut des Lizenzvertrags erhalten Sie beim Kauf und bei Installation eines Kaspersky Lab Programms das Recht, Ihre Kopie fristlos zu benutzen.

Kaspersky Lab wird Ihnen auch gerne zusätzlichen Service leisten:

- Technischer Support;
- Update von Kaspersky Anti-Viren-Datenbanken;
- Update von Kaspersky Anti-Virus-Programmmodulen.

Um diesen Service zu erhalten, müssen Sie eine Lizenz kaufen und aktivieren.

ÜBER DIE KASPERSKY ANTI-VIRUS-LIZENZEN

Lizenz – ist ein Recht auf die Anwendung von Kaspersky Anti-Virus und den dazu gehörendem zusätzlichen Service, den Ihnen Kaspersky Lab oder seine Partner leisten.

Jede Lizenz wird durch Typ und Laufzeit gekennzeichnet.

Lizenzlaufzeit – ist der Zeitabschnitt während dessen Ihnen der zusätzliche Service gewährleistet wird. Der Serviceumfang hängt vom Lizenztyp ab.

Es sind folgende Lizenztypen vorgesehen:

Testlizenz – eine kostenlose Lizenz mit beschränkter Laufzeit. Eine solche Lizenz ist zum kennenlernen von Kaspersky Anti-Virus bestimmt. Sie wird zusammen mit der Testversion des Programms geliefert und hat eine kurze Laufzeit. Bei der Anwendung dieser Lizenz können Sie sich nicht an den technischen Support wenden. Sobald die Laufzeit abgelaufen ist, stellt Kaspersky Anti-Virus alle seine Funktionen ein.

Gewerbliche Lizenz – entgeltliche Lizenz, deren Laufzeit in der Regel nicht weniger als 1 Jahr beträgt. Solche Lizenzen werden dem Benutzer beim Kauf des Programms übergeben. Nach dem Ablauf der Laufzeit der gewerblichen Lizenz führt Kaspersky Anti-Virus alle seinen Funktionen weiter aus. Nur der zusätzliche Service wird nicht mehr gewährleistet.

Um in den Genuss des Programms und den zusätzlichen Service zu kommen, müssen Sie eine gewerbliche Lizenz kaufen und aktivieren.

Die Lizenzaktivierung wird durch Installation der Schlüsseldatei durchgeführt.

ÜBER DIE KASPERSKY ANTI-VIRUS-SCHLÜSSELDATEI

Schlüsseldatei – ist ein technisches Mittel, mit welcher die Aktivierung der mit ihr zusammenhängenden Lizenz ermöglicht.

Die Schlüsseldatei ist im Lieferumfang enthalten, insofern Sie diese über einen Kaspersky Lab Distributor beziehen, oder wird Ihnen per Post zugeliefert, falls das Programm im Online-Shop gekauft wird.

Eine Schlüsseldatei enthält folgende Informationen:

- Lizenzlaufzeit.
- Lizenztyp (Testlizenz, gewerbliche Lizenz).
- Lizenzbeschränkungen (z. B. für wie viele Computer die Lizenz gilt oder der Umfang des geschützten E-Mail-Verkehrs).
- Kontaktinformation für Anfragen an den technischen Support.
- Gültigkeitsdauer der Schlüsseldatei.

Gültigkeitsdauer der Schlüsseldatei – ist ein Recht auf die Anwendung von Kaspersky Anti-Virus und den dazu gehörendem zusätzlichen Service, den Ihnen Kaspersky Lab oder seine Partner leisten. Dies meint den Zeitraum, nach dessen Ablauf die Schlüsseldatei nicht mehr gilt und dementsprechend die Möglichkeit der mit ihm zusammenhängenden Lizenzaktivierung verloren geht.

Lassen Sie uns an einem Beispiel betrachten, wie die Gültigkeitsdauer der Schlüsseldatei und die der Lizenz zusammenhängen.

Beispiel:

Lizenzlaufzeit: 300 Tage

Ausstellungdatum der Schlüsseldatei: 11.01.2010

Laufzeit der Schlüsseldatei: 300 Tage

Installationsdatum der Schlüsseldatei (Lizenzaktivierung): 20.01.10, d. h. 9 Tage nach dem Ausstellungsdatum.

Ergebnis:

Berechnete Lizenzlaufzeit: 300 Tage-9 Tage = 291 Tage.

INSTALLATION DER SCHLÜSSELDATEI

Die Installation der Schlüsseldatei wird für jeden einzelnen Server separat ausgeführt. Sie können zwei Schlüsseldateien installieren: Eine aktive und eine zusätzliche (Reservelizenz). Die aktive Schlüsseldatei wirkt gleich nach der Installation. Im Programm kann nicht mehr als eine aktive Schlüsseldatei installiert werden. Eine zusätzliche Schlüsseldatei tritt nach dem Ablauf der Laufzeit der aktiven Schlüsseldatei in Kraft. Die Schlüsseldateien können während der Kaspersky Anti-Virus Installationsprozedur installiert werden.

Vor der Installation der Schlüsseldatei durch die Oberfläche der Domino-Server-Konsole, überzeugen Sie sich bitte davon, dass die Schlüsseldatei auf dem Dateisystem des Servers, auf welchem diese installiert wird, verfügbar ist. Bei der Installation der Schlüsseldatei durch einen Lotus Notes Client oder durch einen Web-Browser, überzeugen Sie sich bitte davon, dass er auf dem Dateisystem des Clientcomputers, auf dem die Verwaltungscenter Datenbank geöffnet wurde, verfügbar ist.

Um eine Schlüsseldatei zu installieren, handeln Sie wie folgt:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Wählen Sie im Profilbestand des Navigation panels den Server aus, für welchen Sie die Schlüsseldatei installieren möchten.
3. Im Verwaltungsfeld wählen Sie den **Lizenz** Tab (s. Abbildung unten).
4. Betätigen Sie die Schaltfläche **Schlüsseldatei hinzufügen**.
5. Im geöffneten Fenster wählen Sie die Schlüsseldatei mit der Dateiendung .key und betätigen danach die **Öffnen** Schaltfläche.

   Als Folge wird die angegebene Schlüsseldatei auf dem Server installiert (s. Abbildung unten).

Im **Lizenz** Tab können Sie folgende Informationen über die installierte Lizenz einsehen:

- **Funktion**. Es gibt folgende mögliche Einschränkungen der Funktionalität:
  - **Vollständig** – die Lizenz ist installiert worden.
  - **Nur Verwaltung** – die Lizenz ist nicht installiert worden oder die Gültigkeitsdauer der Testlizenz ist abgelaufen.
  - **Nur Update** – beim Anti-Viren-Datenbanken-Update ist ein Fehler aufgetreten, Die Anti-.Viren-Datenbanken sind beschädigt oder die Lizenz ist in der Schwarzen Liste hinterlegt.
  - **Vollständig ohne Updates** – Die Laufzeit der gewerblichen Lizenz ist abgelaufen.

- **Typ**. Lizenztyp (Testlizenz, gewerbliche Lizenz).
- **Ablaufdatum des Gültigkeitszeitraumes**. Ablaufdatum der Lizenzlaufzeit.
- **Verbleibende Zeit (Tage)**. Dauer, während der Sie zusätzlichen Service genießen.
- **Lizenznummer**. Lizenzseriennummer.
- **Besitzerdaten**. Information über den Lizenzbesitzer: Organisation, Besitzername, Land, E-Mail-Adresse usw.

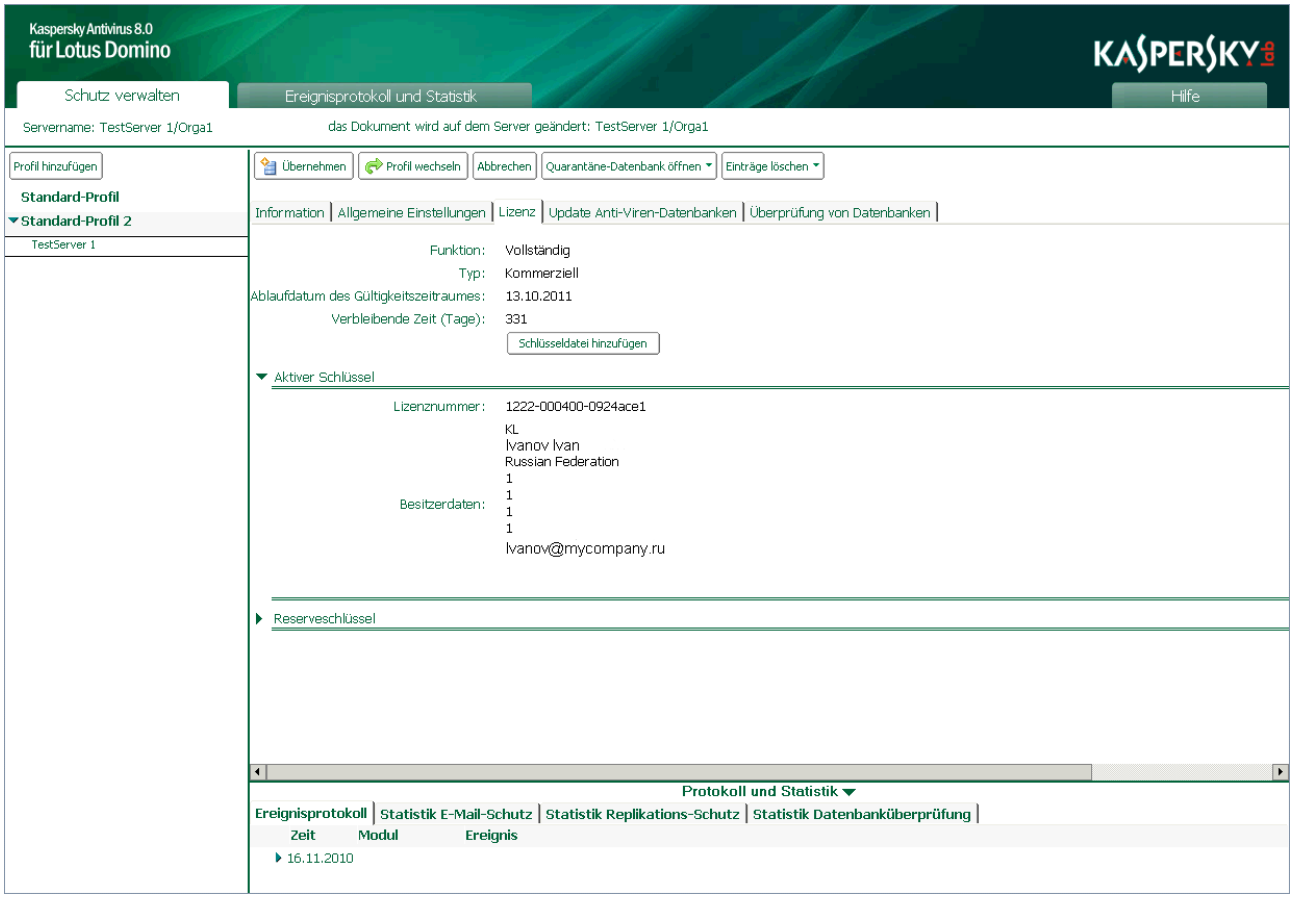


Abbildung 2: Informationen über die installierte Lizenz einsehen

Eine aktive bzw. zusätzliche Schlüsseldatei kann nur durch die Befehlszeile gelöscht werden (s. Abschnitt "Server-Konsole-Modus" auf der S. 122).

PROGRAMMOBERFLÄCHE

In diesem Abschnitt werden die Hauptelemente der Kaspersky Anti-Virus Oberfläche beschrieben.

Alle Operationen zu Einstellung und Verwaltung von Kaspersky Anti-Virus werden durch die Benutzeroberfläche der Verwaltungscenter Datenbank ausgeführt. Im Fenster der Verwaltungscenter Datenbank können Sie auch mit den Quarantäne-, Ereignisprotokoll-, Statistik- und Hilfe-Datenbanken arbeiten.

Der Zugriff zu den Datenbanken ist durch einen Lotus Notes Client auch durch einen Web-Browser möglich. Die Web-Oberfläche ermöglicht es, das Programm von Computern aus zu verwalten, auf denen Lotus Notes Client nicht installiert ist.

Es ist auch ein Befehlssatz zur Verwaltung von Kaspersky Anti-Virus durch eine Domino-Server-Konsole vorgesehen (s. Abschnitt "Server-Konsole-Modus" auf der S. 122).

Über die benötigten Rechte zum Öffnen der kavcontrolcenter.nsf Datenbank, zur Einstellungsanpassung oder zur Verwaltung von Kaspersky Anti-Virus verfügen nur jene Benutzer, welche die Berechtigungen einer der drei Funktionsgruppen besitzen: **Sicherheitsadministratoren**, **ControlCenter-Administratoren** und **Administratoren mit eingeschränkten Berechtigungen**. Vor der Datenbanköffnung überzeugen Sie sich bitte davon, dass das Benutzerkonto die Berechtigungen zur Ausführung der nötigen Aktionen besitzt.

Die Fensterstruktur der Verwaltungscenter Datenbank und den Aktionen bei der Operationsausführung sind bei der Arbeit via Lotus Notes Client und über Web-Browser identisch. Deshalb wird in allen folgenden Abschnitten dieses Handbuchs die Arbeit mit Kaspersky Anti-Virus durch Lotus Notes Client beschrieben.

Um das Fenster der Verwaltungscenter Datenbank zu öffnen, wählen Sie eine der folgenden Vorgehensweisen:

- Öffnen Sie mit Hilfe des Lotus Notes Client die Datenbank kavcontrolcenter.nsf auf einem der Server, auf welchem Kaspersky Anti-Virus installiert ist;
- Öffnen Sie einen Browser und geben Sie in der Adressenzeile ein:

  `http://<Servername>/<Dateipfad_kavcontrolcenter.nsf>?OpenDatabase`

  wobei:

  - `<Servername>` – Name oder IP-Adresse des Servers, auf dem Kaspersky Anti-Virus installiert ist;
  - `<Dateipfad_kavcontrolcenter.nsf>` – kavcontrolcenter.nsf - Dateipfad des Datenkatalogs des Servers.

Als Folge wird das Fenster der Verwaltungscenter Datenbank geöffnet (s. Abbildung unten).

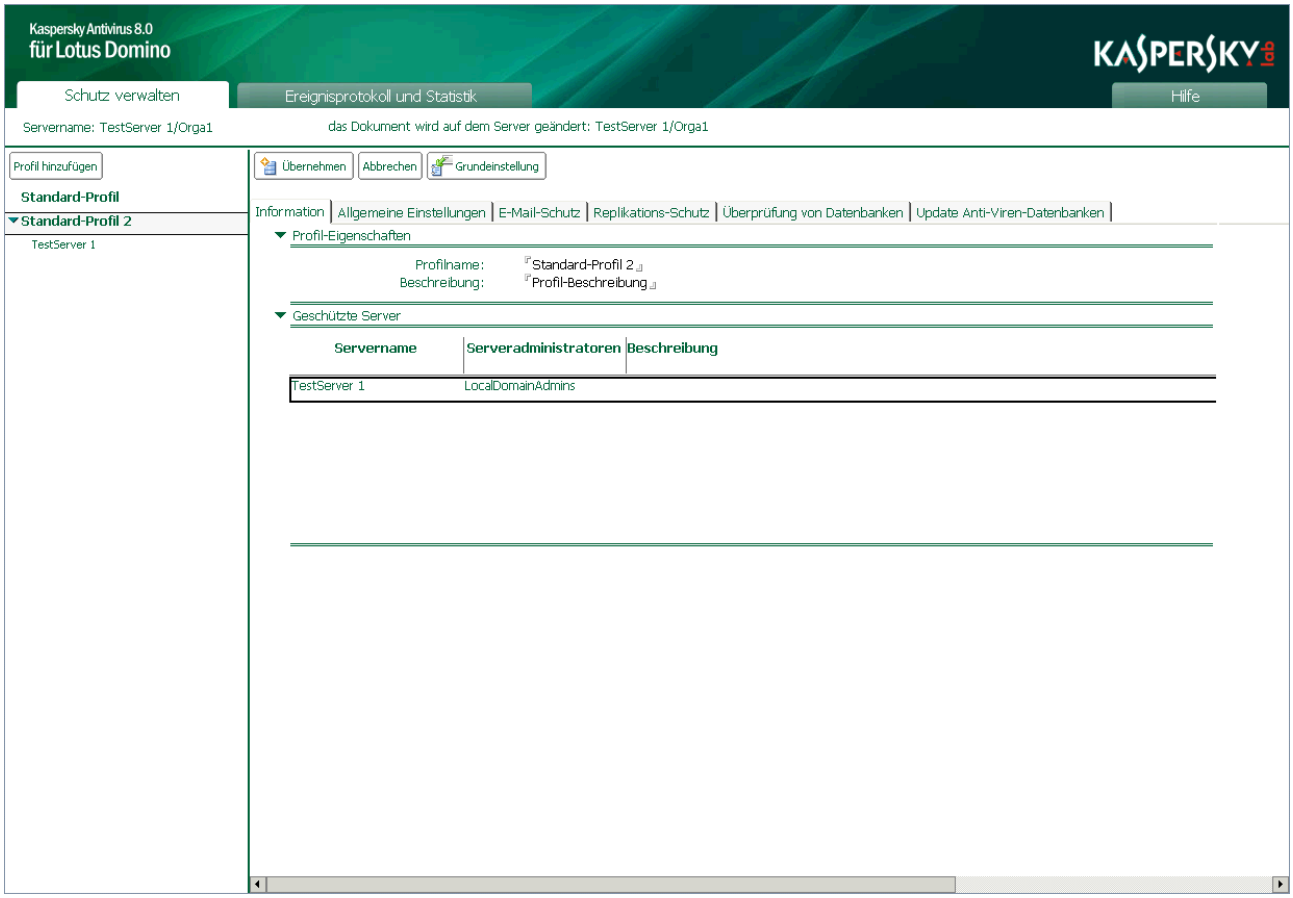


Abbildung 3: Fenster der Verwaltungscenter Datenbank

Hier und nachstehend werden Bilder eines mit Lotus Notes Client geöffneten Fensters der Verwaltungscenter Datenbank dargestellt.

Beim ersten Öffnen der Verwaltungscenter Datenbank wird im Arbeitsbereich von Lotus Notes automatisch ein Shortcut erstellt. Der Shortcut kann im Weiteren zum öffnen des Fensters der Verwaltungscenter Datenbank verwendet werden.

Im Fall der Arbeit mit Kaspersky Anti-Virus durch einen Web-Browser kann der Zugriffspfad zu kavcontrolcenter.nsf Datenbank gespeichert und im Weiteren zum aufrufen des Fensters der Verwaltungscenter Datenbank verwendet werden.

IN DIESEM ABSCHNITT

Fensterstruktur der Verwaltungscenter Datenbank 40

Schutzverwaltung Tab 41

Ereignisprotokoll und Statistik Tab 44

Hilfe Tab 45

FENSTERSTRUKTUR DER VERWALTUNGSCENTER DATENBANK

Das Fenster der Verwaltungscenter Datenbank besteht aus folgenden Hauptelementen (s. Abbildung unten):

- *Switch panel* – befindet sich im oberen Fensterteil und enthält Tabs für Umschaltung zwischen dem Verwaltungscenter, den Ereignisprotokoll-, Statistik- und Hilfedatenbanken.
- *Statusfeld* – befindet sich im oberen Fensterteil, enthält den Namen des Servers, zu welchem man verbunden ist, und den Namen des Servers, auf dem das Dokument geändert wird.

  Bei der Arbeit via Lotus Notes Client kann sich der Server, auf welchem ein Replikat der Verwaltungscenter Datenbank bearbeitet wird, vom dem Server, mit welchem man verbunden ist, unterscheiden (s. Abschnitt "Verwendung der Option der direkten Bearbeitung der Servereinstellungen" auf der S. 118).

- *Navigationsfeld* – befindet sich im linken Fensterteil, je nachdem welcher Tab im Schaltfeld ausgewählt wird, enthält es folgende Bestandteile:
  - Liste von Profilen und zugehörigen Servern;
  - Liste von Ereignisprotokoll und Statistik Abschnitten;
  - Inhaltverzeichnis vom Kaspersky Anti-Virus Hilfesystem.

- *Verwaltungs-* und *Ansichtsbereich* – befinden sich im rechten Fensterteil und sind für die Arbeit mit den Einstellungen von Profilen / Servern, Kaspersky Anti-Virus Datenbankeinträgen sowie zur Durchsicht des Kaspersky Anti-Virus Hilfesystems bestimmt.

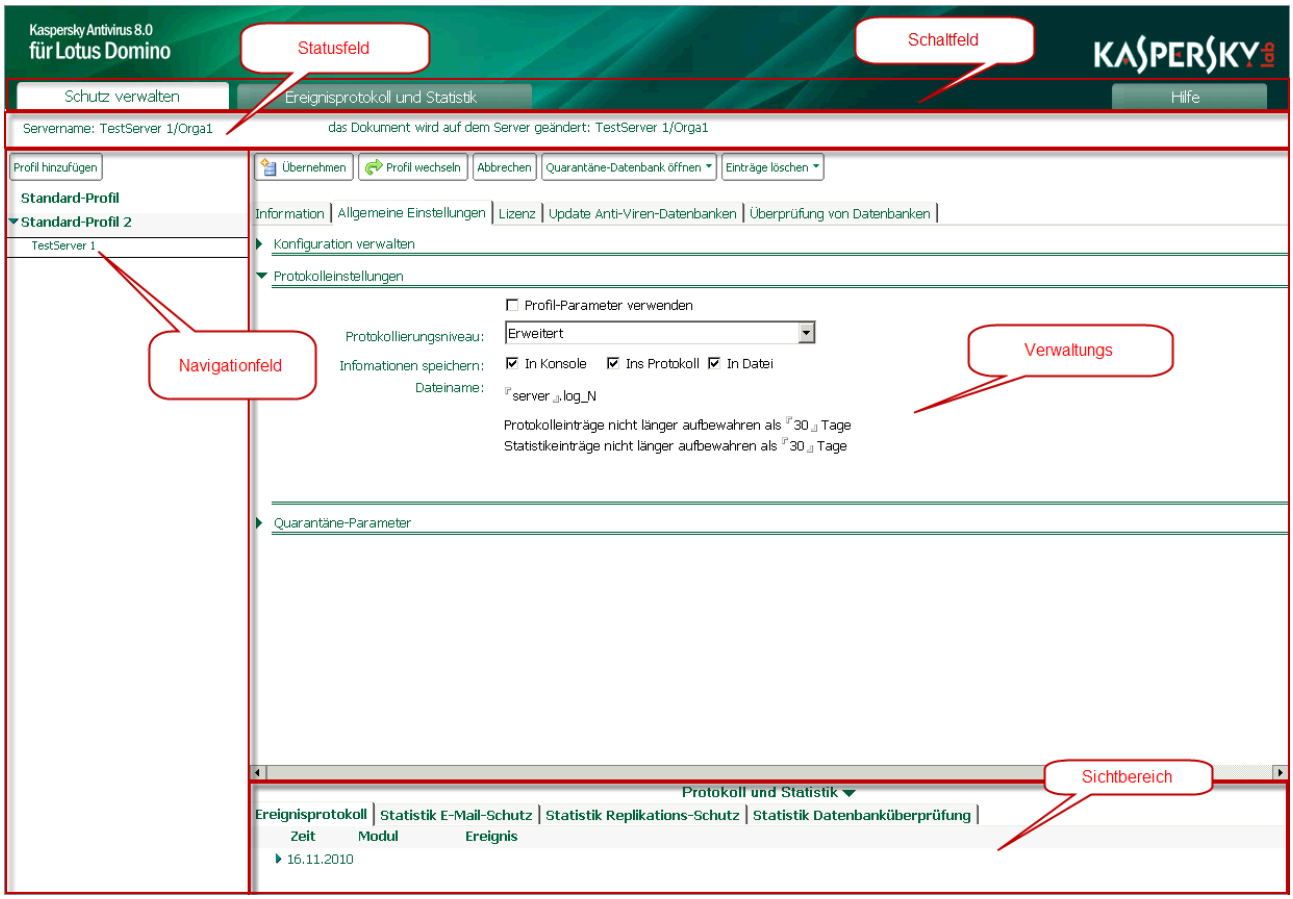


Abbildung 4: Fensterstruktur der Verwaltungscenter Datenbank

Inhalt des Navigationsfeldes. Der Verwaltungs- und Ansichtsbereich hängt davon ab, welcher Tab im Schaltfeld ausgewählt wird.

Die Verfügbarkeit der Oberflächen-Elemente und Eingabefelder im Fenster der Verwaltungscenter Datenbank wird mit dem Berechtigungsumfang des jeweiligen Benutzers bestimmt.

SCHUTZVERWALTUNG TAB

Schutz verwalten. Dieser Tab ist für die Arbeit mit der Verwaltungscenter Datenbank bestimmt: Die Anpassung der Einstellungen von Kaspersky Anti-Virus auf den geschützten Servern und Einstellungsanpassung des Anti-Viren-Schutzes (E-Mail- und Replikationsschutz, Untersuchung von Datenbanken, Anti-Viren-Datenbanken-Update usw.).

Im **Schutz verwalten** Tab enthält das Navigationsfeld eine Liste von Profilen und dazugehörenden Servern.

Die Liste der zum Profil dazugehörenden Server kann im Navigationsfeld zusammengeklappt werden. Um die Serverliste zu öffnen, betätigen Sie das ▸ Zeichen links des Profilnamens.

Im oberen Teil des Navigationsfeldes befindet sich die Schaltfläche **Profil hinzufügen**, die zur Profilerstellung bestimmt ist(s. Abschnitt "Profile erstellen und löschen" auf der S. 112).

Falls im Navigationsfeld ein Profil ausgewählt wird, werden im Verwaltungsbereich folgende Tabs (s. Abbildung unten), die Profilparameter enthalten, dargestellt:

- **Information**. Der Tab enthält den Profilnamen und die Liste der zu dem dazugehörenden Servern.
- **Allgemeine Einstellungen**. Im Tab werden die Namen des Administrators / der Administratorengruppe des Profils, die Einstellungen der Programmleistung (s. Abschnitt "Leistung" auf der S. 89), die Einstellungen des Ereignisprotokolls und der Statistik für die zum Profil gehörenden Server dargestellt (s. Abschnitt "Einstellungen des Ereignisprotokolls" auf der S. 99).
- **E-Mail-Schutz**. Der Tab ist für die Einstellungsanpassung des E-Mail-Schutzes der zum Profil gehörenden Server bestimmt (s. S. 59).
- **Replikations-Schutz**. Der Tab ist zur Einstellungsanpassung des Replikationsschutzes der zum Profil gehörenden Server bestimmt (s. Abschnitt "Replikationsschutz" auf der S. 71).
- **Überprüfung von Datenbanken**. Der Tab ist für die Einstellungsanpassung des E-Mail-Schutzes der zum Profil gehörenden Server bestimmt (s. S. 78).
- **Update Anti-Viren-Datenbanken**. Der Tab ist zur Einstellungsanpassung des Replikationsschutzes der zum Profil gehörenden Server bestimmt (s. Abschnitt "Updatequelle auswählen" auf der S. 55).

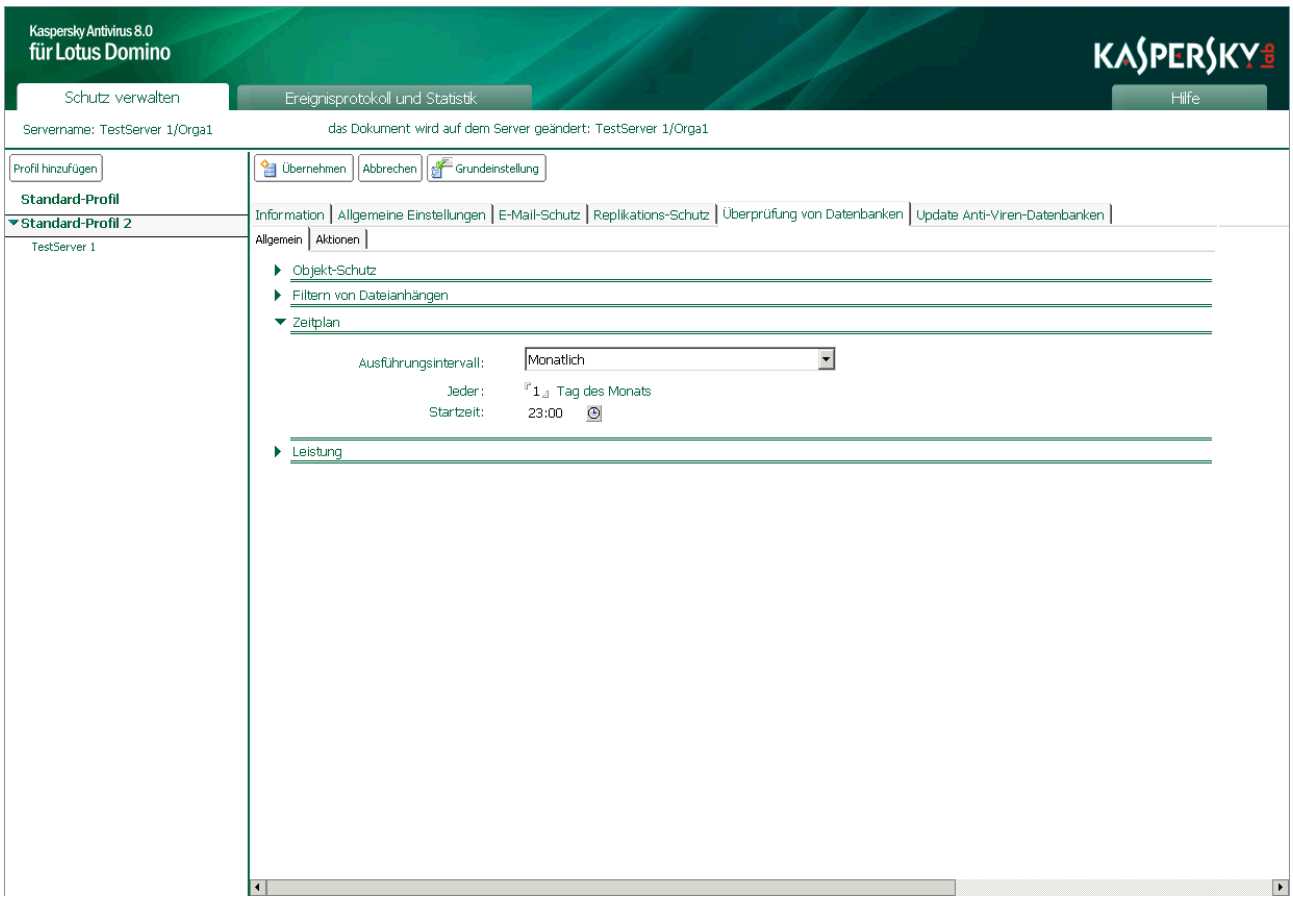


Abbildung 5: Fenster der Verwaltungscenter Datenbank im Modus der Profileinstellungsansicht

Falls im Navigationsfeld ein Server ausgewählt wird, werden im Verwaltungsbereich die Tabs, welche die Servereinstellungen enthalten, dargestellt, und im Ansichtsbereich werden Einträge der Ereignisprotokoll- und Statistikdatenbank für diesen Server dargestellt (s. Abbildung unten).

Falls im Tab **Allgemeine Einstellungen** im Bereich **Konfiguration verwalten** eines Dokuments das Häkchen **Dokument auf dem geschützten Server ändern** gesetzt ist, wird das Dokument aus dem Replikat der Datenbank, das sich auf dem Zielserver befindet, geöffnet.

Im Client der Version 8 und höher wird das Dokument per Mausklick auf das Dokument in der Navigationsleiste geöffnet.

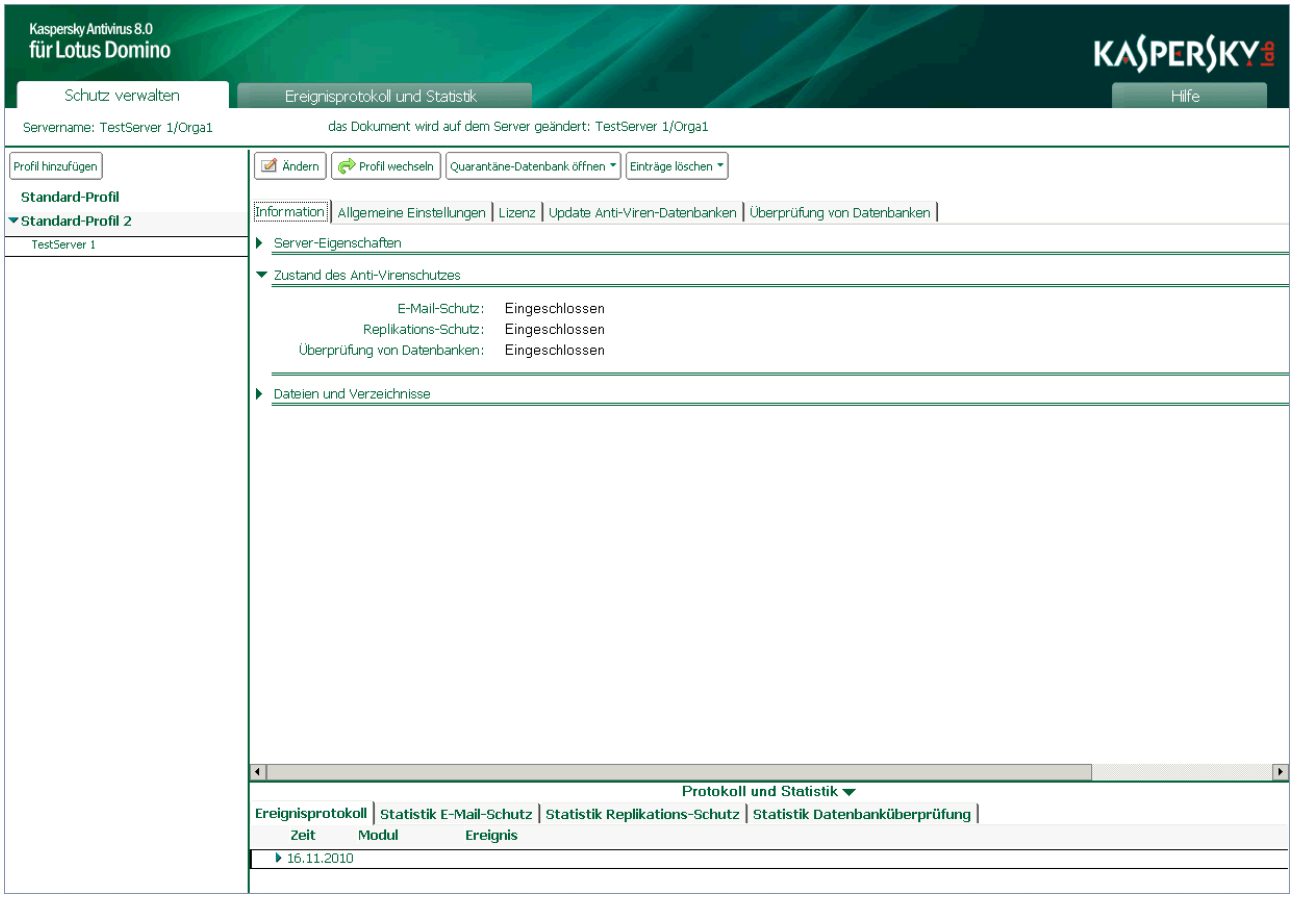


Abbildung 6: Fenster der Verwaltungscenter Datenbank im Ansichtsmodus der Servereinstellungen

Serverparameter sind in folgenden Tabs dargestellt (s. Abbildung oben):

- **Information**. Im Tab wird der Servername, der Name vom Administrator / von der Administratorengruppe des Servers, der Status der Schutzkomponenten dargestellt (s. Abschnitt "Serverschutzzustand" auf der S. 47).

- **Allgemeine Einstellungen**. Im Tab sind Quarantäne-Einstellungen(s. Abschnitt "Quarantäne-Einstellungen" auf der S. 96), einzelne Einstellungen des Ereignisprotokolls und der Statistik für den Server dargestellt (s. Abschnitt "Einstellungen des Ereignisprotokolls" auf der S. 99).

- **Lizenzen**. Der Tab ist für Lizenzverwaltung bestimmt(s. Abschnitt "Lizenzverwaltung" auf der S. 34).

- **Update Anti-Viren-Datenbanken**. Der Tab ist für Einstellung von Update-Parametern der Antiviren-Datenbanken für Server(s. Abschnitt "Updatequelle" auf der S. 52) und Update-Start bestimmt (s. Abschnitt "Manuelles Update" auf der S. 58).

- **Überprüfung von Datenbanken**. Der Tab ist für Start der manuellen Untersuchung von Datenbanken für Server bestimmt(s. Abschnitt "Manuelle Untersuchung" auf der S. 87).

Im oberen Teil des Verwaltungsbereichs wird das Aktionsfeld, das Befehltasten enthält, dargestellt.

Um Profil- bzw. Serverparameter bearbeiten zu können, soll man auf die Schaltfläche **Ändern**, die sich im Aktionsfeld befindet, vom Modus des Parameterdurchsehens zum Bearbeitungsmodus übergehen. Im Aktionsfeld unterscheidet sich der Tastenbestand im Bearbeitungsmodus von dem im Ansichtsmodus.

Bestimmung der Tasten, die sich bei der Arbeit mit Profilparametern im Aktionsfeld befinden, wird in der Tabelle unten angeführt.

Tabelle 4. Tasten im Aktionsfeld bei der Arbeit mit Profilparametern

SCHALTFLÄCHE	BESTIMMUNG
Ändern	Zum Profilparameter Bearbeitungsmodus übergehen.
Übernehmen	Änderungen der Profilparameter speichern.
Abbrechen	Ausgeführte Änderungen abbrechen.
Löschen	Profil löschen.
Grundeinstellung	Die als standardmäßige vorgesehenen Profilparameter wiederherstellen.

Bestimmung der Tasten, die sich bei der Arbeit mit Serverparametern im Aktionsfeld befinden, wird in der Tabelle unten angeführt.

Tabelle 5. Tasten im Aktionsfeld bei der Arbeit mit Serverparametern

SCHALTFLÄCHE	BESTIMMUNG
Ändern	Zum Serverparameter Bearbeitungsmodus übergehen.
Übernehmen	Änderungen der Serverparameter speichern.
Profil vertauschen	Server zum Bestand vom anderen Profil verschieben.
Abbrechen	Ausgeführte Änderungen abbrechen.
Quarantäne-Datenbank öffnen	Die Liste von Objekten, die als Folge der E-Mail-, Replikations- und Datenbankenuntersuchung in Quarantäne verschoben wurden, öffnen (s. S. 91).
Einträge löschen	Quarantäne-Einträge löschen (s. Abschnitt "Aktionen an den in die Quarantäne verschobenen Objekte" auf der S. 94) oder Einträge des Ereignisprotokolls und die Statistik jeweiliger Server löschen (s. Abschnitt "Löschen der Information aus der Ereignisprotokoll- und Statistikdatenbank" auf der S. 104).

EREIGNISPROTOKOLL UND STATISTIK TAB

Der **Ereignisprotokoll und Statistik** Tab ist für die Arbeit mit der Ereignisprotokoll- und Statistikdatenbank bestimmt: D. h. dies lässt Sie Informationen über Ereignisse, die beim Programmdurchlauf auf allen geschützten Servern registriert wurden, statistische Information über die während der Anti-Viren-Untersuchung entdeckten Bedrohungen und daran ausgeführten Aktionen einsehen (s. Abschnitt "Die Ereignisprotokoll- und Statistikdatenbank einsehen" auf der S. 105).

Im **Ereignisprotokoll und Statistik** Tab des Navigation panels existiert eine Liste mit Teilen und Abschnitten des Ereignisprotokolls und der Statistik, und im Sichtbereich des rechten Fensterteils werden Einträge der Ereignisprotokoll- und Statistikdatenbank dargestellt (s. Abbildung unten).

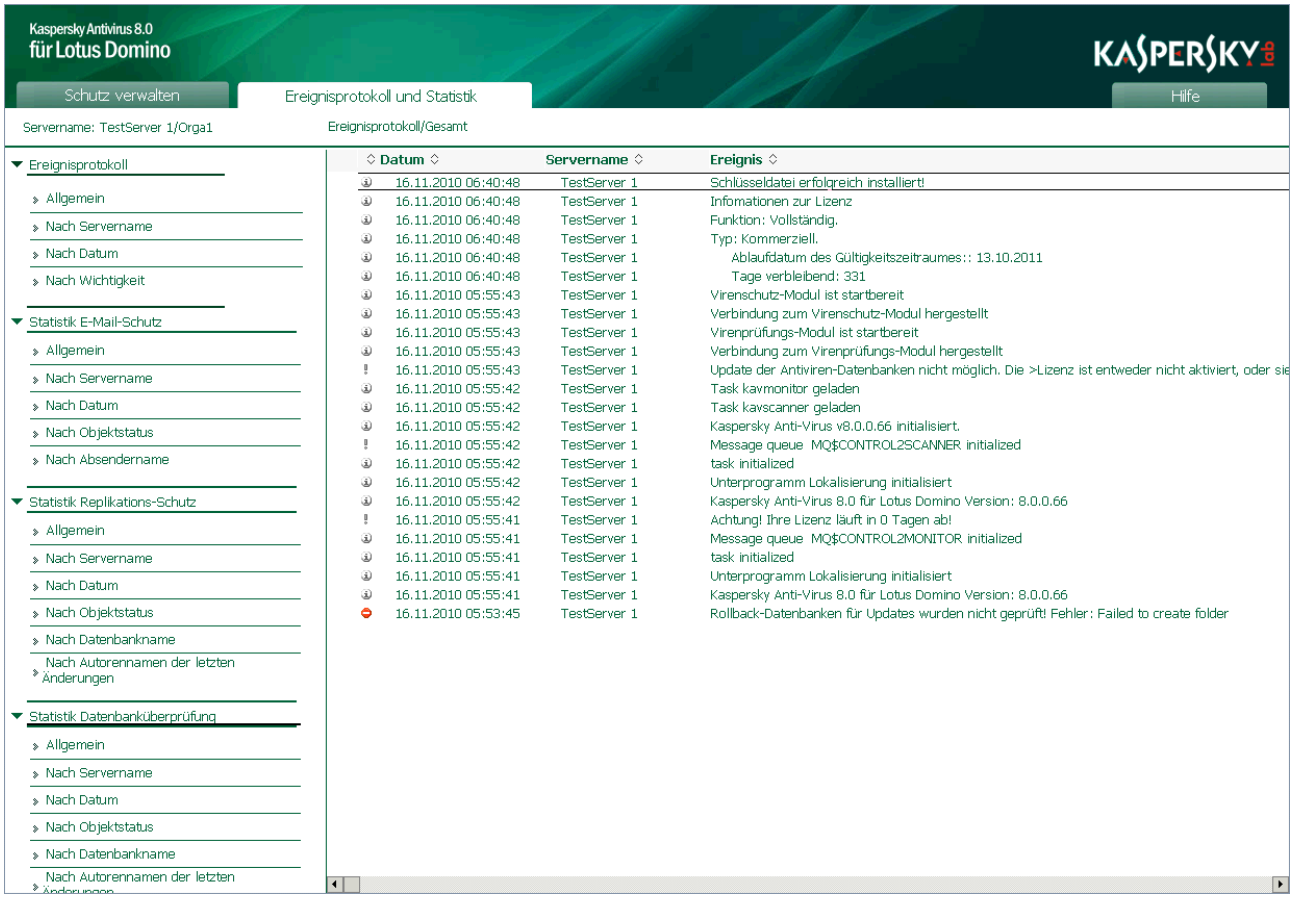

Kaspersky Antivirus 8.0
für Lotus Domino
KASPERSKY lab
Schutz verwalten
Ereignisprotokoll und Statistik
Hilfe
Servername: TestServer 1/Orga1
Ereignisprotokoll/Gesamt
Ereignisprotokoll
Allgemein
Nach Servername
Nach Datum
Nach Wichtigkeit
Statistik E-Mail-Schutz
Allgemein
Nach Servername
Nach Datum
Nach Objektstatus
Nach Absendername
Statistik Replikations-Schutz
Allgemein
Nach Servername
Nach Datum
Nach Objektstatus
Nach Datenbankname
Nach Autorennamen der letzten Änderungen
Statistik Datenbanküberprüfung
Allgemein
Nach Servername
Nach Datum
Nach Objektstatus
Nach Datenbankname
Nach Autorennamen der letzten
Datum
Servername
Ereignis
16.11.2010 06:40:48 TestServer 1 Schlüsseldatei erfolgreich installiert!
16.11.2010 06:40:48 TestServer 1 Infomationen zur Lizenz
16.11.2010 06:40:48 TestServer 1 Funktion: Vollständig.
16.11.2010 06:40:48 TestServer 1 Typ: Kommerziell.
16.11.2010 06:40:48 TestServer 1 Ablaufdatum des Gültigkeitszeitraumes:: 13.10.2011
16.11.2010 06:40:48 TestServer 1 Tage verbleibend: 331
16.11.2010 05:55:43 TestServer 1 Virenschutz-Modul ist startbereit
16.11.2010 05:55:43 TestServer 1 Verbindung zum Virenschutz-Modul hergestellt
16.11.2010 05:55:43 TestServer 1 Virenprüfungs-Modul ist startbereit
16.11.2010 05:55:43 TestServer 1 Verbindung zum Virenprüfungs-Modul hergestellt
16.11.2010 05:55:43 TestServer 1 Update der Antiviren-Datenbanken nicht möglich. Die >Lizenz ist entweder nicht aktiviert, oder sie
16.11.2010 05:55:42 TestServer 1 Task kavmonitor geladen
16.11.2010 05:55:42 TestServer 1 Task kavscanner geladen
16.11.2010 05:55:42 TestServer 1 Kaspersky Anti-Virus v8.0.0.66 initialisiert.
16.11.2010 05:55:42 TestServer 1 Message queue MQ$CONTROL2SCANNER initialized
16.11.2010 05:55:42 TestServer 1 task initialized
16.11.2010 05:55:42 TestServer 1 Unterprogramm Lokalisierung initialisiert
16.11.2010 05:55:42 TestServer 1 Kaspersky Anti-Virus 8.0 für Lotus Domino Version: 8.0.0.66
16.11.2010 05:55:41 TestServer 1 Achtung! Ihre Lizenz läuft in 0 Tagen ab!
16.11.2010 05:55:41 TestServer 1 Message queue MQ$CONTROL2MONITOR initialized
16.11.2010 05:55:41 TestServer 1 task initialized
16.11.2010 05:55:41 TestServer 1 Unterprogramm Lokalisierung initialisiert
16.11.2010 05:55:41 TestServer 1 Kaspersky Anti-Virus 8.0 für Lotus Domino Version: 8.0.0.66
16.11.2010 05:53:45 TestServer 1 Rollback-Datenbanken für Updates wurden nicht geprüft! Fehler: Failed to create folder

Abbildung 7: Das Fenster der Verwaltungscenter Datenbank im Ansichtsmodus des Ereignisprotokolls und der Statistik

HILFE TAB

Der **Hilfe** Tab ist zur Durchsicht der Hilfe Datenbank bestimmt.

Im Navigation panel des **Hilfe** Tabs befindet sich ein Inhaltsverzeichnis des Kaspersky Anti-Virus Hilfesystems. Im rechten Fensterteil wird die Hilfeinformation im Sichtbereich dargestellt.

PROGRAMM STARTEN UND BEENDEN

Kaspersky Anti-Virus wird beim Domino-Server-Start automatisch gestartet. Der Anti-Viren-Schutz startet nach der Kaspersky Anti-Virus Installation und dem Neustart des Servers.

Sie können Kaspersky Anti-Virus mit der Befehlszeile der Domino-Server-Konsole starten sowie anhalten (s. Abschnitt "Server-Konsole-Modus" auf der S. 122).

SERVERSCHUTZZUSTAND

Der Serverschutz besteht aus folgenden Komponenten: Den E-Mail-Schutz, den Replikationsschutz und die Untersuchung der Datenbanken. Standardmäßig sind alle Schutzkomponenten aktiviert und werden beim Domino-Server-Start automatisch gestartet. Vom Tage der Installation ab wird die Untersuchung der Datenbanken einmal pro Monat um 23:00 Uhr gestartet.

Um Informationen über aktivierte und deaktivierte Schutzkomponenten zu erhalten gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Navigation panelWählen Sie einen Server aus dem Profilbestand im Navigation panel, dessen Schutzzustand Sie überprüfen wollen.

3. Im Verwaltungsbereich wählen Sie den **Information** Tab. Der Status der Schutzkomponenten wird im Bereich Status des **Zustand des Anti-Virenschutzes** (s. Abbildung unten).

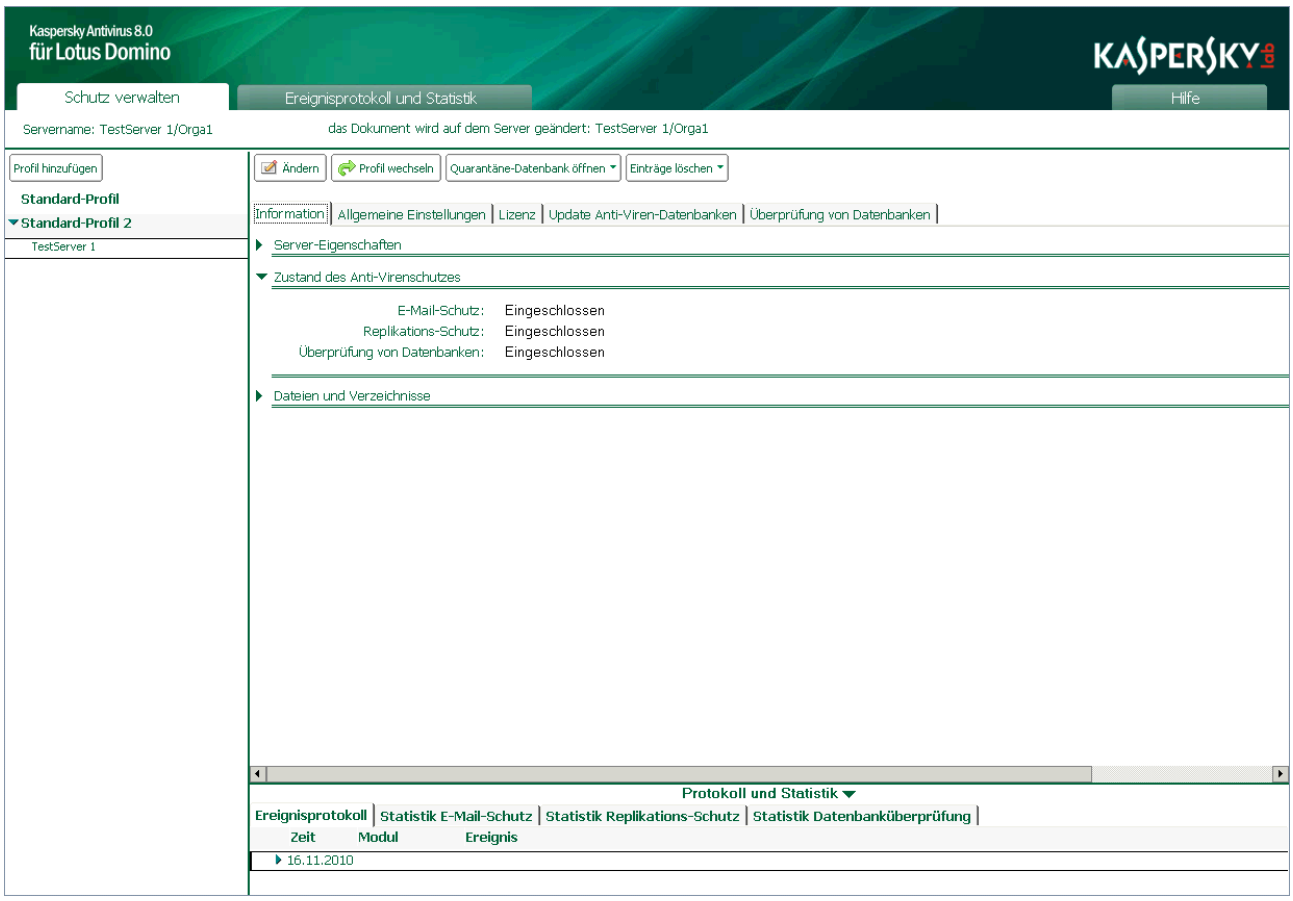


Abbildung 8: Fenster der Verwaltungscenter Datenbank im Ansichtsmodus der Servereinstellungen

Sie können jede Schutzkomponente aktivieren unddeaktivieren.

Um eine Schutzkomponente zu aktivieren oder deaktivieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie im Profilbestand einen Server, für welchen Sie eine Schutzkomponente aktivieren oderdeaktivieren möchten.
3. Betätigen Sie im Action panel die **Ändern** Schaltfläche und im Verwaltungsbereich wählen Sie den Tab: **Information** (s. Abbildung oben).
4. Wählen Sie im Bereich **Zustand des Anti-Virenschutzes** aus der, der jeweiligen Komponente entsprechenden Zeile, eine der Varianten: **Aktivieren** oder **Deaktivieren**.
5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

STANDARDMÄßIGER SERVERSCHUTZ

Der Anti-Viren-Schutz startet nach der Installation von Kaspersky Anti-Virus und dem Neustart des Servers. Alle Programmmodule und Schutzkomponenten werden beim Server-Start automatisch mitgestartet. Standardmäßig führt Kaspersky Anti-Virus folgende Aktionen aus:

- Untersucht den E-Mail-Verkehr. Bei der Untersuchung werden folgende Parameterwerte verwendet:
    - E-Mail-Bodys, Anhänge und OLE-Objekte werden untersucht;
    - Desinfizierbare Objekte behandeln, nicht desinfizierbare, möglicherweise infizierte und verdächtige Objekte löschen;
    - Einzelne Objekte nicht länger als 300 Millisekunden untersuchen;
    - Objekte bis 1024 KB werden im Serverarbeitsspeicher untersucht ohne auf der Festplatte gespeichert zu werden;
    - Objektkopien in die Quarantäne verschieben;
    - Speichern von Informationen über entdeckte Objekte und die ausgeführten Aktionen in der Ereignisprotokoll- und Statistikdatenbank;
    - Hinzufügen von Informationsmeldungen in den E-Mail-Body;
    - In den Betreff der E-Mail wird die Kennzeichnung **Überprüft durch Kaspersky Anti-Virus für Lotus Domino hinzugefügt**;
    - Im Falle einer Entdeckung von zehn infizierten Objekten im Laufe einer Stunde wird eine Nachricht über die Bedrohung einer Epidemieentstehung gesendet.
- Alle neuen und infolge der Replikation geänderten Dokumente werden untersucht. Bei der Untersuchung werden folgende Parameterwerte verwendet:
    - Felder der RTF-Dokumente, Anhänge und OLE-Objekte untersuchen;
    - Desinfizierbare Objekte behandeln, nicht desinfizierbare, möglicherweise infizierte und verdächtige Objekte löschen;
    - Einzelne Objekte nicht länger als 300 Millisekunden untersuchen;
    - Objekte bis 1024 KB werden im Serverarbeitsspeicher untersucht ohne auf der Festplatte gespeichert zu werden;
    - Objektkopien in die Quarantäne verschieben;
    - Speichern von Informationen über entdeckte Objekte und die ausgeführten Aktionen in der Ereignisprotokoll- und Statistikdatenbank;
    - Senden von Informationsmeldungen an die Administratoren, bezügl.
- Untersuchung der Datenbanken. Planmäßig wird die Untersuchung täglich um 23:00 gestartet. Bei der Untersuchung werden folgende Parameterwerte verwendet:
    - Felder der RTF-Dokumente, Anhänge und OLE-Objekte untersuchen;
    - Untersuchung der Datenbanken, welche sich im Root des data Ordners befinden mit allen seinen Unterordnern;

  - Ausschluss der Quarantäne-Datenbank aus der Untersuchung;
  - Desinfizierbare Objekte behandeln, nicht desinfizierbare, möglicherweise infizierte und verdächtige Objekte löschen;
  - Einzelne Objekte nicht länger als 300 Millisekunden untersuchen;
  - Objekte bis 1024 KB werden im Serverarbeitsspeicher untersucht ohne auf der Festplatte gespeichert zu werden;
  - Objektkopien in die Quarantäne verschieben;
  - Speichern von Informationen über entdeckte Objekte und die ausgeführten Aktionen in der Ereignisprotokoll- und Statistikdatenbank;
  - Senden von Informationsmeldungen an die Administratoren, bezügl. ausgeführter Aktionen

- Speichert die von Kaspersky Anti-Virus Arbeit registrierten Ereignisse im Ereignisprotokoll und der Statistik und sendet diese an die Domino-Server-Konsole. Detailgenauigkeit – erweitert. Ereignisse und statistische Information über die Ergebnisse der Objektuntersuchung werden in der Ereignisprotokoll- und Statistikdatenbank für 30 Tage gespeichert.
- Startet das planmäßige Update der Anti-Viren-Datenbanken täglich um 23:00 Uhr. Als Updatequelle werden die Server von Kaspersky Lab verwendet.

UPDATE DER DATENBANKEN

Kaspersky Anti-Virus sucht nach bösartigen Programmen und behandelt infizierte Objekte mit Hilfe der Anti-Viren-Datenbank-Einträge. Es ist höchst wichtig, die Anti-Virus-Datenbanken im aktuellen Status zu halten, denn neue Viren, Trojaner und andere bösartige Programme erscheinen täglich. Wir empfehlen die Anti-Viren-Datenbanken gleich nach der Programminstallation aktualisieren zu lassen, denn die Datenbanken, welche in den Distribution enthalten sind, verlieren bis zum Installationszeitpunkt an Aktualität. Das Update der Anti-Viren-Datenbanken wird für jeden einzelnen Server separat gestartet.

Auf den Kaspersky Lab Servern werden Anti-Virus-Datenbanken stündlich aktualisiert. Information zur Aktualität der von Kaspersky Anti-Virus verwendeten Anti-Viren-Datenbanken, können Sie in den Servereinstellungen im **Update der Anti-Viren-Datenbanken** Tab finden.

➧ *Um Information über die Anti-Viren-Datenbanken, die von Kaspersky Anti-Virus verwendet werden, zu erhalten, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Wählen Sie im Profilbestand des Navigation panels den Server, dessen Informationen Sie einsehen wollen.

3. Im Verwaltungsbereich wählen Sie den **Update der Anti-Viren-Datenbanken** Tab.

Information über die von Kaspersky Anti-Virus verwendeten Anti-Viren-Datenbanken wird im oberen Tabteil dargestellt.

Kaspersky Anti-Virus kopiert die Updates der Anti-Viren-Datenbanken via Internet von den Kaspersky Lab Update-Servern oder von anderweitigen FTP / HTTP-Servern bzw, vom Administrator bestimmte Netzwerkressourcen. Die erhaltenen Updates werden auf dem Server im Programmdienstordner kavcommon\updater (kavcommon/updater – für Linux) abgelegt. Dieser Ordner wird bei der Programminstallation erstellt und befindet sich unter folgendem Pfad:

- Für Betriebssysteme der Microsoft Windows Reihe – im Binärdateienordner des Domino-Servers (standardmäßiger Pfad: C:\Program Files\IBM\Lotus\Domino);

- Für Betriebssysteme der Linux Reihe – im Datenkatalog des Domino-Servers (standardmäßiger Pfad: /local/notesdata).

Die von einem der Server erhaltenen Updates können für weitere Instanzen von Kaspersky Anti-Virus genutzt werden, welche sich auf weiteren Servern befinden. Dafür muss der Dienstordner kavcommon\updater\retranslation (kavcommon/updater/retranslation – für Linux) als Updatequelle angegeben werden, der sich auf dem Server – Updatequelle unter folgender Adresse befindet:

- Für Betriebssysteme der Microsoft Windows Reihe – im Binärdateienordner des Domino-Servers (standardmäßiger Pfad: C:\Program Files\IBM\Lotus\Domino);

- Für Betriebssysteme der Linux Reihe – im Datenkatalog des Domino-Servers (standardmäßiger Pfad: /local/notesdata).

Wenn Kaspersky Anti-Virus also auf mehreren Servern installiert ist, kann einer der Server die Updates via Internet kopieren, und die übrigen können ihre Updates von diesem Server beziehen (s. Abschnitt "Update-Schema" auf der S. 53).

Beim Update-Prozess werden die Anti-Viren-Datenbanken auf dem Server mit jenen in der Updatequelle befindlichen Antiviren-Datenbanken von Kaspersky Anti-Virus verglichen. Falls der Anti-Viren-Datenbank-Bestand unterschiedlich ist, wird der fehlende Teil von der Updatequelle kopiert. Datenbanken werden nicht vollständig kopiert, wodurch sich die Updategeschwindigkeit wesentlich steigert und der Netzwerkverkehr entlastet werden kann.

Vor dem Update erstellt Kaspersky Anti-Virus eine Sicherheitskopie der Anti-Viren-Datenbanken. Falls der Download der Updates abgebrochen oder mit einem Fehler beendet wird, stellt Kaspersky Anti-Virus die Anti-Viren-Datenbanken aus der Sicherheitskopie wieder her. Tritt während des Betriebs von Kaspersky Anti Viruseine Beschädigung der Anti-Viren-Datenbanken auf, stellt Kaspersky Anti-Virus die Anti-Viren-Datenbanken aus der Sicherheitskopie, die beim letzten Update erstellt wurde, wieder her.

Updates werden entweder planmäßig oder manuell aktualisiert. Informationen über Ereignisse, die im Betrieb von Kaspersky Anti-Virus während eines Updates registriert wurden, werden in der Ereignisprotokoll- und Statistikdatenbank gespeichert (s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98).

Sie können die Update-Einstellungen mehrerer Server durch den Einsatz eines Profils konfigurieren oder individuelle Update-Einstellungen für jeden einzelnen Server einstellen (s. Abschnitt "Kaspersky Anti-Virus Einstellungsverwaltung" auf der S. 26).

IN DIESEM ABSCHNITT

Updatequelle 52

Update-Schema 53

Updatequelle auswählen 55

Planmäßiges Update 56

Manuelles Update 58

UPDATEQUELLE

Die *Updatequelle* ist eine Ressource, die Updates der Kaspersky Anti-Viren-Datenbanken enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner dienen.

Als Hauptquelle des Kaspersky Lab Programm-Updates gelten Kaspersky Lab Update-Server. Die sind spezielle Internet-Seiten, auf welchen Updates aller Programme von Kaspersky Lab hinterlegt werden.

Falls Sie keinen Zugriff auf den Kaspersky-Lab-Updateserver haben (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unter den Telefonnummern +7 (495) 797-87-00 und +7 (495) 645-79-39 unsere Zentrale anrufen. Dort können Sie sich nach den Adressen der Partner von Kaspersky Lab, die Ihnen Updates auf Wechseldatenträgern im zip-Format anbieten können, erkundigen.

Auf Wechseldatenträgern erhaltene Updates können Sie auf beliebige FTP / HTTP-Server oder auch in einem lokalen- oder Netzwerkordner hinterlegen.

Als Updatequelle von Kaspersky Anti-Virus für Lotus Domino kann auch der auf einem anderen geschützten Server gespeicherte Dienstordner dienen – kavcommon\updater\retranslation\ (kavcommon/updater/retranslation – für Linux).

UPDATE-SCHEMA

Falls Kaspersky Anti-Virus nur auf einem Server installiert ist, können Sie die Updates von den Kaspersky Lab Update-Servern oder irdendeiner anderen Quelle, welche die Anti-Viren-Datenbanken Updates enthalten, herunterladen: FTP / HTTP-Server, lokale- oder Netzwerkordner (s. Abbildung unten).

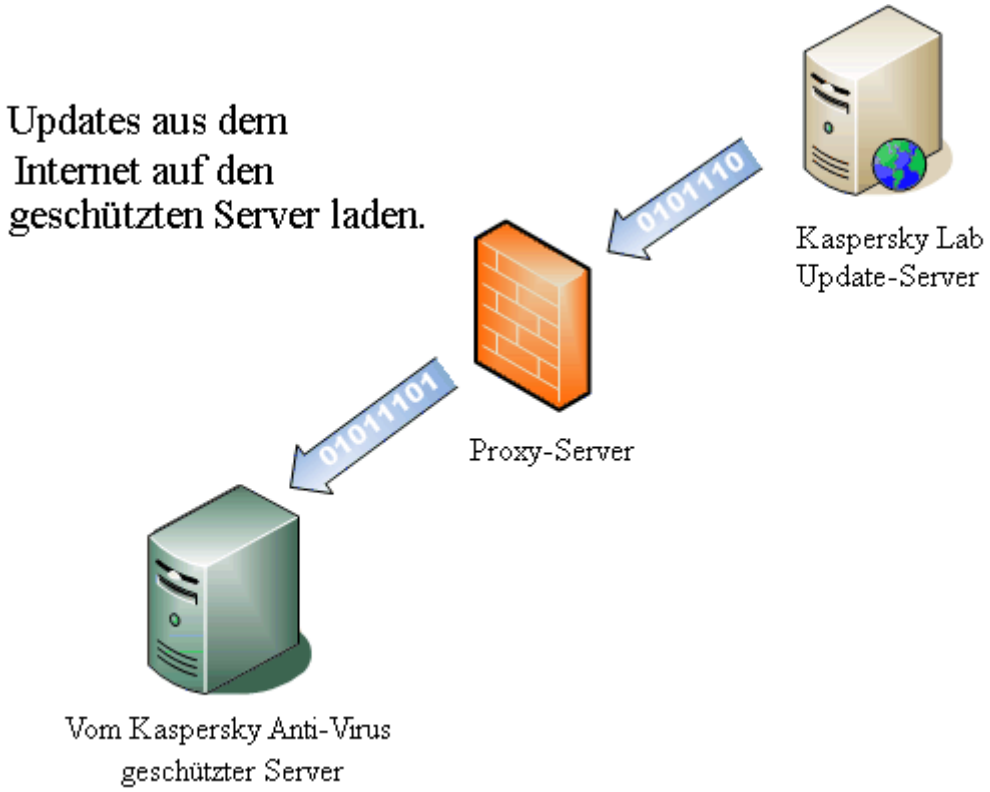


Abbildung 9: Schema eines Updates über das Internet von Kaspersky Lab Servern

Falls Kaspersky Anti-Virus auf mehreren Servern installiert ist, können Sie folgende Update-Schemen verwenden:

- verteilt – Updates werden für jeden geschützten Server direkt aus dem Internetheruntergeladen (s. Abbildung oben);

- integriert – Updates werden aus dem Internet auf einen Server heruntergeladen. Die übrigen Server verbinden sich zu diesem Server, auf welchem die für Kaspersky Anti-Virus erhaltenen Updates hinterlegt sind (s. Abbildung unten).

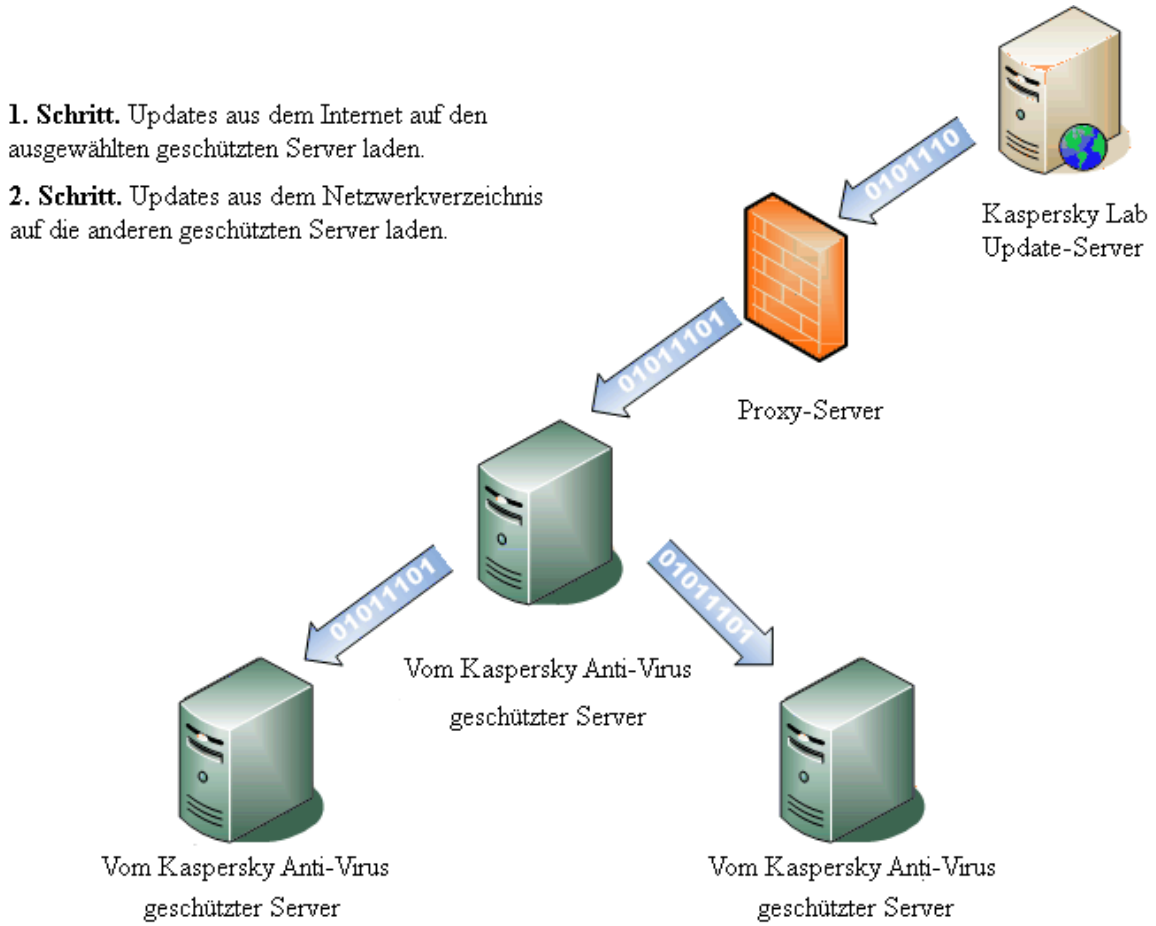

1. Schritt. Updates aus dem Internet auf den ausgewählten geschützten Server laden.
2. Schritt. Updates aus dem Netzwerkverzeichnis auf die anderen geschützten Server laden.
01011101
Kaspersky Lab Update-Server
01011101
Proxy-Server
01011101
01011101
Vom Kaspersky Anti-Virus geschützter Server
Vom Kaspersky Anti-Virus geschützter Server
Vom Kaspersky Anti-Virus geschützter Server

Abbildung 10: Zentralisiertes Update-Schema

Um ein integriertes Update-Schema zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie den Server, der die Updatesdurch das Internet erhalten wird und als Update-Quelle für andere Server verwendet wird. In den Update-Einstellungen dieses Servers geben Sie als Updatequelle die Update-Server von Kaspersky Lab an(s. Abschnitt "Updatequelle auswählen" auf der S. 55).

2. Ermöglichen Sie allen Servern, welche von diesem ausgewählten Server aktualisiert werden, den Lesezugriff auf den auf diesem Server gespeicherten Ordner kavcommon\updater\retranslation (kavcommon/updater/retranslation – für Linux).

3. Als Updatequelle geben Sie für alle Server, welche von diesem Server aktualisiert werden, den Ordner kavcommon\updater\retranslation (kavcommon/updater/retranslation – für Linux) an.

Bei Verwendung eines zentralisierten Update-Schemas, wird empfohlen, den Parameter KAVCustomUpdUrlOnly=1 in der notes.ini für alle Server, welche diesem ausgewählten Server aktualisiert werden, zu setzen.

UPDATEQUELLE AUSWÄHLEN

Update-Einstellungen können für eine Server-Gruppe und für einzelne Server bestimmt werden. Um eine einheitliche Updatequelle für eine Server-Gruppe anzugeben, verwenden Sie die Profileinstellungen. Um eine Updatequelle für einen einzelnen Server anzugeben, verwenden Sie die Servereinstellungen.

Um eine Updatequelle an zugeben, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Wählen Sie das Profil im Navigation panel , falls Sie die Update-Einstellungen für eine Server-Gruppe anpassen wollen, oder den Server, wenn Sie die Update-Einstellungen für einen einzelnen Server einstellen möchten.

3. Betätigen Sie die **Ändern** Schaltfläche aus dem Action panel und wählen den **Update Anti-Viren-Datenbanken** Tab im Verwaltungsbereich (s. Abbildung unten).

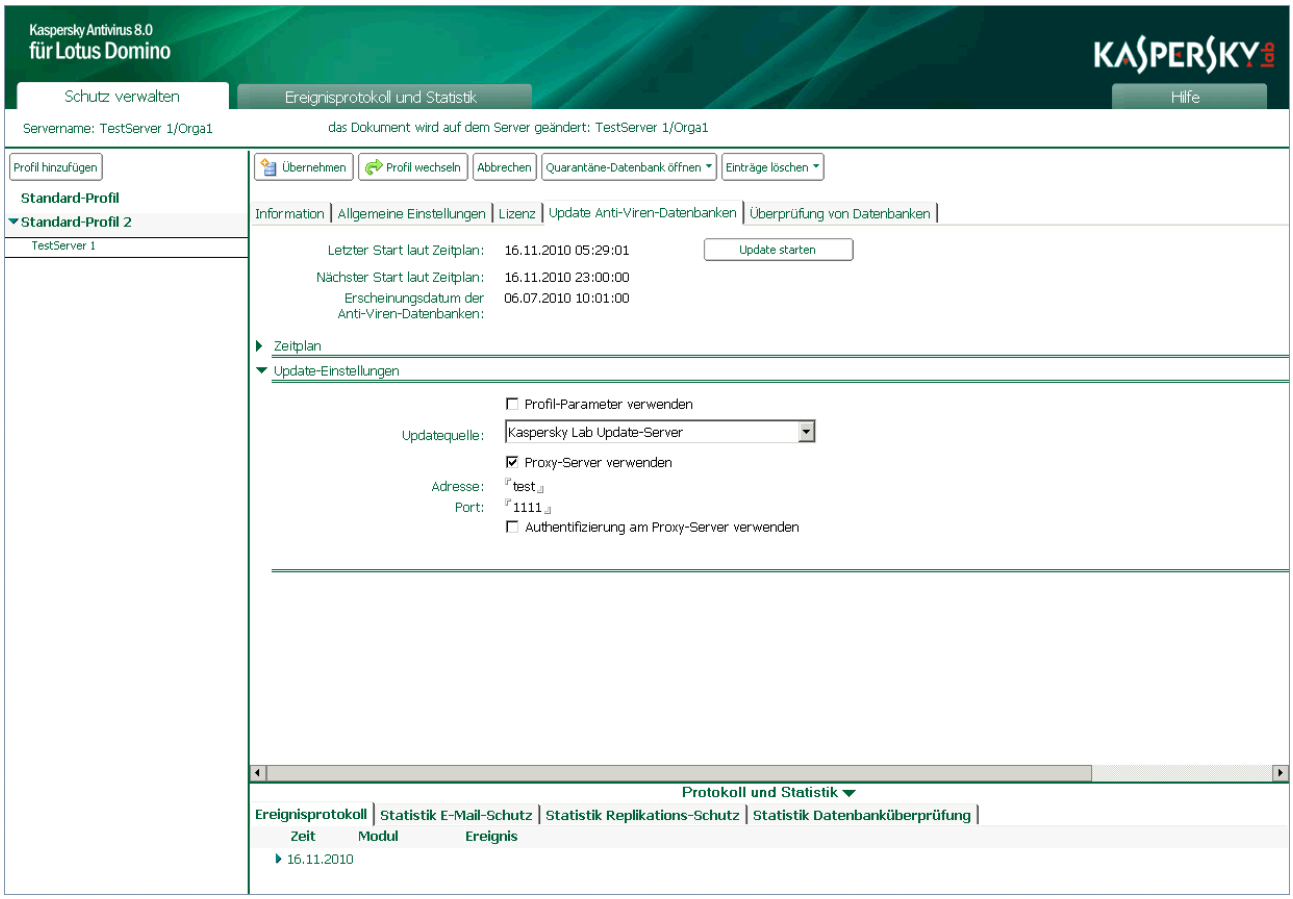


Abbildung 11: Auswahl der Update-Quelle

Falls Sie die Update-Einstellungen für einen Server anpassen möchten, entfernen Sie im **Update-Einstellungen** Bereich das Häkchen **Profil-Einstellungen verwenden**. Falls das Häkchen gesetzt ist, können die Update-Einstellungen nicht geändert werden. Wollen Sie, dass die über das Profil angegebenen Einstellungen verwendet werden, muss das Häkchen **Profil-Parameter verwenden** gesetzt werden.

4. Geben Sie die Updatequelle ein. Dafür wählen Sie im **Bereich Update-Einstellungen** in der **Updatequelle einen** der folgenden Werte:

- **Kaspersky Lab Update-Server** – als Update-Quelle werden die Internet-Seiten von Kaspersky Labverwendet. Die vorgegebene Quelle ist standardmäßig eingestellt.

- **Andere HTTP- und FTP-Server oder Netzwerkressourcen** – als Update-Quelle wird die Ressource, die im Feld **URL-Adresse** (in den Profileinstellungen) / **Adresse der Quelle** (in Serverparametern) eingegeben wird, verwendet. Geben Sie einen FTP / HTTP-Server, einen lokalen- oder Netzwerkordner an. Der Ressourcenpfad muss in UNC-Format (Universal Naming Convention) eingegeben werden.

  Als Updatequellen können FTP-Server mit Authorisierung auftreten.HTTP-Server welche eine Authorisierung erwarten, können nicht als Updatequellen verwendet werden.

  Wollen Sie, die Updates von einem Kaspersky Anti-Virus Dienstordner auf einem anderen geschützten Server kopieren lassen, geben Sie in diesem Feld den Pfad zum Ordner kavcommon\updater\retranslation (kavcommon/updater/retranslation – für Linux) an. Für Betriebssysteme der Microsoft Windows-Reihe wird der Ordnerpfad bezüglich des Binärdateienordners des Domino-Servers angegeben (standardmäßig: C:\Program Files\IBM\Lotus\Domino). Für Betriebssysteme der Linux-Reihe wird der Ordnerpfad bezüglich des Dateienordners des Domino-Servers eingegeben (standardmäßig – /local/notesdata).

Falls es dem Server nicht gelingt, ein Update von der vorgegebenen Quelle auszuführen, versucht Kaspersky Anti-Virus sich mit einer andere Update-Quelle zu verbinden– Dabei wird versucht, sich an die Ressource zu wenden, von welcher das letzte erfolgreiche Update ausgeführt wurde oder an den Kaspersky Lab Update-Server. Damit der Server sich nur von der von Ihnen vorgegebenen Updatequelle aktualisiert, muss der Parameter KAVCustomUpdUrlOnly in der Konfigurationsdatei notes.ini gesetzt werden (s. Abschnitt "Einstellungsverwaltung der Konfigurationsdatei notes.ini" auf der S. 28): KAVCustomUpdUrlOnly=1.

5. Falls die Verbindung zur Update-Ressource durch einen Proxy-Server hergestellt wird, passen Sie die Einstellungen für den Proxy-Server an. Dazu gehen Sie wie folgt vor:

   - Setzen Sie Häkchen **Proxy-Server verwenden**, im Feld **Adresse**. Geben Sie die IP-Adresse oder den Namen, im **Port** –Feld - die Portnummer des Proxy-Servers an, durch welchen die Verbindung hergestellt wird.

   - Setzen Sie das Häkchen **Authentifizierung am Proxy-Server verwenden**, falls bei der Verbindung zum angegebenen Proxy-Server eine Benutzer-Authentifizierung durchgeführt wird. Füllen Sie **Benutzer** und **Kennwort**-Felder aus.

6. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Falls Sie die Update-Einstellungen für eine Server-Gruppe anpassen möchten, können Sie die standardmäßigen Einstellungswerte wiederherstellen. Dazu betätigen Sie die Schaltfläche **Grundeinstellung**.

PLANMÄßIGES UPDATE

Kaspersky Anti-Virus führt das Anti-Viren-Datenbank-Update nach einem Update-Plan aus. Sie können den gleichen Zeitplan für eine Server-Gruppe durch ein Profil vorgeben oder via Servereinstellungen einzelne Zeitpläne für einen beliebigen Server einstellen.

➧ *Um den Update-Plan für einen Server oder eine Server-Gruppe zu erstellen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, wenn Sie die Update-Einstellungen für eine Server-Gruppe einstellen wollen, oder den Server, falls Sie Update-Einstellungen für einen einzelnen Server anpassen möchten.

3. Betätigen Sie die **Ändern** Schaltfläche aus dem Action panel und wählen den Update der **Anti-Viren-Datenbanken** Tab im Verwaltungsbereich (s. Abbildung unten).

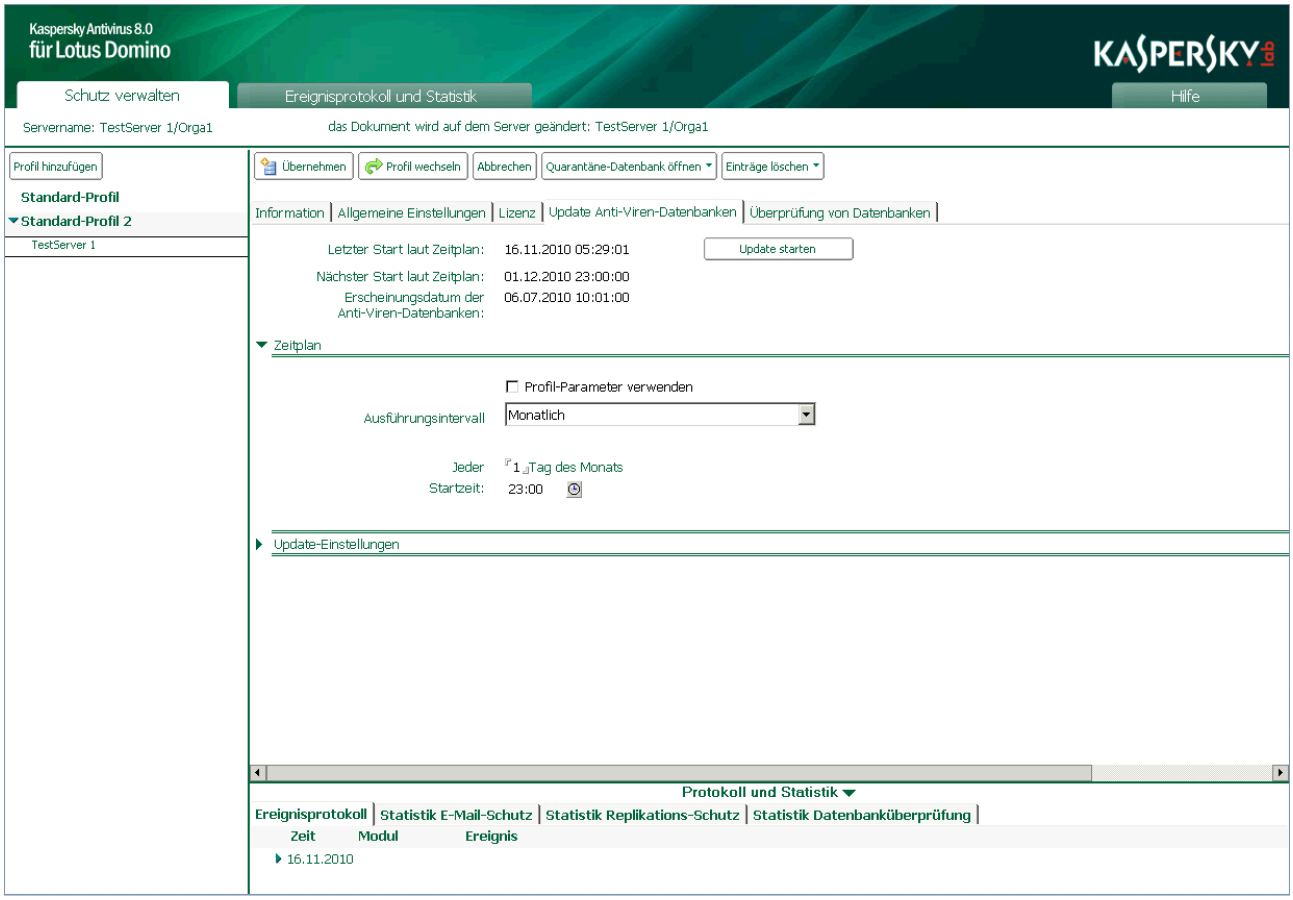


Abbildung 12: Einstellung des Zeitplans des Updates der Anti-Viren-Datenbanken

Falls Sie die Update-Einstellungen für einen Server anpassen möchten, entfernen Sie im **Update-Einstellungen** Bereich das Häkchen **Profil-Einstellungen verwenden**. Falls das Häkchen gesetzt ist, können die Update-Einstellungen nicht geändert werden. Wollen Sie, dass die über das Profil angegebenen Einstellungen verwendet werden, muss das Häkchen **Profil-Parameter verwenden** gesetzt werden.

4. Im Bereich **Zeitplan** wählen Sie in der geöffneten **Ausführungsintervall** - Liste eine der folgenden Angaben:

   - **Täglich** – das Update wird täglich mit dem in Stunden eingegebenen Intervall ausgeführt. Die standardmäßige Uhrzeit desersten Starts beträgt 23:00 Uhr.

   - **Monatlich** – das Update wird einmal pro Monat am angegeben Tag zur angegebenen **Startzeit** ausgeführt. Geben Sie die nötige Angabe im Feld **Startzeit** ein. Format **Std.:Min**.

     Falls es im Monat weniger Tage als vorgegeben gibt, wird das Update am letzten Tag des Monats ausgeführt.

   - **Wöchentlich** – das Update wird wöchentlich zu den angegebenen Tagen in der eingegebenen **Startzeit** ausgeführt. Setzen Sie das Häkchen an den Wochentagen, an welchen das Update gestartet werden soll und geben im **Startzeit** Feld die nötigen Angaben an. Format **Std.:Min**.

   - **Manuell** – Ein planmäßiges Update wird nicht ausgeführt. Sie können das Update für einzelne Server mit der Schaltfläche **Update starten** (s. Abschnitt "**Manuelles Update**" auf der S. 58) oder aus der Befehlszeile starten (s. Abschnitt "Server-Konsole-Modus" auf der S. 122).

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Falls Sie die Update-Einstellungen für eine Server-Gruppe anpassen möchten, können Sie die standardmäßigen Einstellungswerte wiederherstellen. Dazu betätigen Sie die Schaltfläche **Grundeinstellung**.

MANUELLES UPDATE

Ein manuelles Update der Anti-Viren-Datenbanken kann nur für einen Server gestartet werden. Für eine Server-Gruppe ist dieser Update-Modus nicht vorgesehen.

Um ein manuelles Update der Anti-Viren-Datenbanken auszuführen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Wählen Sie den Server, dessen Anti-Viren-Datenbanken aktualisiert werden sollen,aus dem Profilbestand im Navigation panel.

3. Wählen Sie den Tab **Update der Anti-Viren-Datenbanken** aus dem Verwaltungsbereich Tab (s. Abbildung unten). Im Tab werden Informationen über Datum und Zeit des letzten und nächsten Starts der Untersuchung der Datenbanken laut den Zeitplänen dargestellt. Sie können dem Update-Verlauf mit Hilfe der Domino-Konsole folgen.

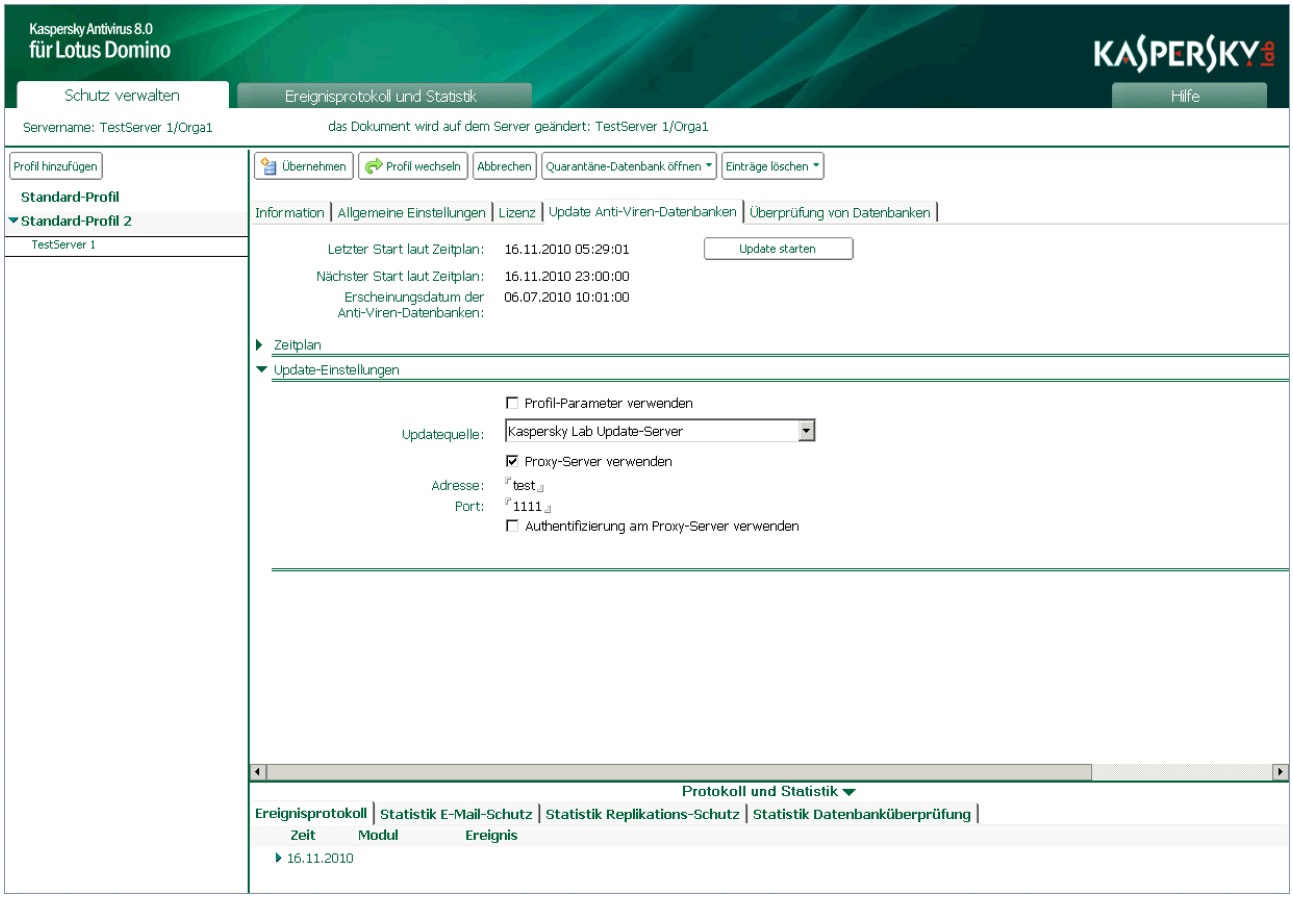


Abbildung 13: Auswahl der Update-Quelle

4. Betätigen Sie die **Update starten Schaltfläche**, um ein Update der Anti-Viren-Datenbanken für einen Server zu starten.

Das Update kann auch aus der Befehlszeile gestartet werden (s. Abschnitt "Arbeit im Server-Konsolen-Modus" auf der S. 122).

E-MAIL-SCHUTZ

Falls der E-Mail-Schutz aktiviert ist (s. Abschnitt "E-Mail-Schutz aktivieren und deaktivieren" auf der S. 60), untersucht und behandelt Kaspersky Anti-Virus möglichst alle auf den Domino-Server ein- und ausgehenden E-Mails und die Durchgangspost.

Während der Untersuchung und Verarbeitung wird die E-Mailzustellung verzögert. Die E-Mails werden in ihre Bestandteile aufgeteilt: E-Mailkörper, Anhänge und OLE-Objekte. Danach werden die Anhänge nach Größe und / oder nach Dateinamen (s. Abschnitt " Algorithmus zur Filterung von Anhängen " auf der S. 24) gefiltert und eine Antiviren-Objektuntersuchung (s. Abschnitt "Algorithmus der Objektuntersuchung auf Vorhandensein von Bedrohungen" auf der S. 24) durchgeführt.

Bei der Überprüfung der E-Mails des Domino-Servers verwendet Kaspersky Anti-Virus den Task `kavmonitor`.

Beim Anhalten des Tasks kavmonitor wird keine Überprüfung der E-Mails durchgeführt. Nicht überprüfte E-Mails werden nicht an die entsprechenden Benutzer gesendet sondern in der Datenbank mail.box abgespeichert.

Damit die Post an ihre Empfänger gesendet wird, muss man den Task `kavmonitor` aktivieren.

Die bei der Untersuchung entdeckten infizierten, möglicherweise infizierten und wegen einer Störung oder Beschädigung nicht untersuchten Objekte werden gemäß den E-Mail-Schutzeinstellungen verarbeitet (s. Abschnitt "Aktionen für E-Mail-Objekte" auf der S. 62). Den Anhänge, deren Größe den angegebenen Wert überschreiteten und / oder deren Namen der angegebenen Dateinamensmaske entsprechen, kann eine besondere Verarbeitungsreihenfolge zugewiesen werden (s. Abschnitt "Filtern von E-Mail-Anhängen" auf der S. 67).

Nach der Programminstallation werden Standardeinstellungen verwendet (s. Abschnitt "Standardmäßiger Serverschutz" auf der S. 49). Sie können sie den gestellten Sicherheitsanforderungen entsprechend anpassen. Ein Teil dieser aufgezählten Einstellungen ist standardmäßig deaktiviert oder kann von einem Administrator deaktiviert werden.

Standardmäßig wird vor der Verarbeitung eine Kopie von der ganzen Meldung oder eine Objektkopie in Quarantäne verschoben (s. Abschnitt "Quarantäne" auf der S. 91).

In den E-Mail Body und Betreff werden Informationen über die Untersuchung durch Kaspersky Anti-Virus und die Beschreibung der ausgeführten Aktionen hinzugefügt. Benachrichtigungen von den bei der Verarbeitung ausgeführten Aktionen werden an Sender/Empfänger und den Administratoren gesendet (s. Abschnitt "Benachrichtigungen" auf der S. 109). Informationen über die Untersuchungsergebnisse und ausgeführten Aktionen werden in die Ereignisprotokoll- und Statistikdatenbanken eingetragen (s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98).

Nach der Objektuntersuchung und -behandlung wird die E-Mail das Lotus Domino System zur Weitergabe zurückgegeben.

Falls der Mechanismus zur Benachrichtigung über Epidemien aktiviert ist, wird bei einer Mengenübersteigeung von entdeckten infizierten, möglicherweise infizierten, beschädigten Objekten und Objekten, welche eine gleichartige Bedrohung aufweisen, meldet Kaspersky Anti-Virus dies den Administratoren und entsprechende Einträge werden in das Ereignisprotokoll geschrieben. Kriterien, nach welchen die Benachrichtigung über eine Epidemie verschickt wird, werden von einem Administrator angegeben (s. Abschnitt "Benachrichtigungen über Epidemien" auf der S. 68).

Sie können die Untersuchung der Anhänge, OLE-Objekte und E-Mail Bodys deaktivieren (s. Abschnitt "Auswahl von Objekten des E-Mail-Schutzes" auf der S. 61). Sie können auch die Untersuchungsdauer einzelner Objekte beschränken, was die gesamte Performance der E-Mailuntersuchung wesentlich steigert (s. Abschnitt "Leistung" auf der S. 89).

Dabei können Objekte, deren Größe den vorgegebenen Wert nicht überschreiten, im Arbeitsspeicher des Servers, ohne auf der Festplatte gespeichert zu werden, untersucht werden (s. Abschnitt "Leistung" auf der S. 89).

Die Einstellungen des E-Mail-Schutzes werden über das Profil, zu welchem der geschützte Server gehört, bestimmt. Die Anpassung einzelner Einstellungen des E-Mail-Schutzes für einen Server ist nicht vorgesehen. Allerdings kann der E-Mail-Schutz nur für jeden einzelnen Server separat aktiviert (deaktiviert) werden (s. Abschnitt "E-Mail-Schutz aktivieren und deaktivieren" auf der S. 60).

Beachten Sie folgende Beschränkungen während des Betriebs von Kaspersky Anti-Virus:

- Die mit einem offenen Schlüssel, welcher dem Empfänger zugehört,verschlüsselten E-Mails werden nicht untersucht.
- In den E-Mails, welche vom Absender signiert wurden, wird die Signatur beim Hinzufügen des Untersuchungsberichts oder beim Ersetzen der Anhänge durch desinfizierte Dateien beschädigt.
- E-Mails im MIME-Format werden in das Rich Text-Format konvertiert, falls im dem Messagebody der Untersuchungsbericht hinzugefügt wird. Dabei kann die Formatierung verletzt werden.

IN DIESEM ABSCHNITT

E-Mail-Schutz aktivieren und deaktivieren 60

Auswahl von Objekten des E-Mail-Schutzes 61

Aktionen an den E-Mail-Objekten 62

Filtern von E-Mail-Anhängen 67

Benachrichtigungen über Epidemien 68

E-MAIL-SCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig ist der E-Mail-Schutz aktiviert und wird beim Hochfahren des Domino-Servers automatisch gestartet. Informationen über den Start der Module, welche den E-Mail-Schutz sichern, werden im Kaspersky Anti-Virus Ereignisprotokoll geschrieben.

Wenn nötig, können Sie den E-Mail-Schutz aktivieren und deaktivieren. Entsprechende Operationen werden für jeden einzelnen Server separat durchgeführt.

Um den E-Mail-Schutz zu aktivieren / deaktivieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie im Profilbestand den Server, für welchen Sie den E-Mail-Schutz deaktivieren wollen.

3. Im Action panel betätigen Sie die **Ändern** Schaltfläche und im Verwaltungsbereich wählen Sie den **Information** Tab (s. Abbildung unten).

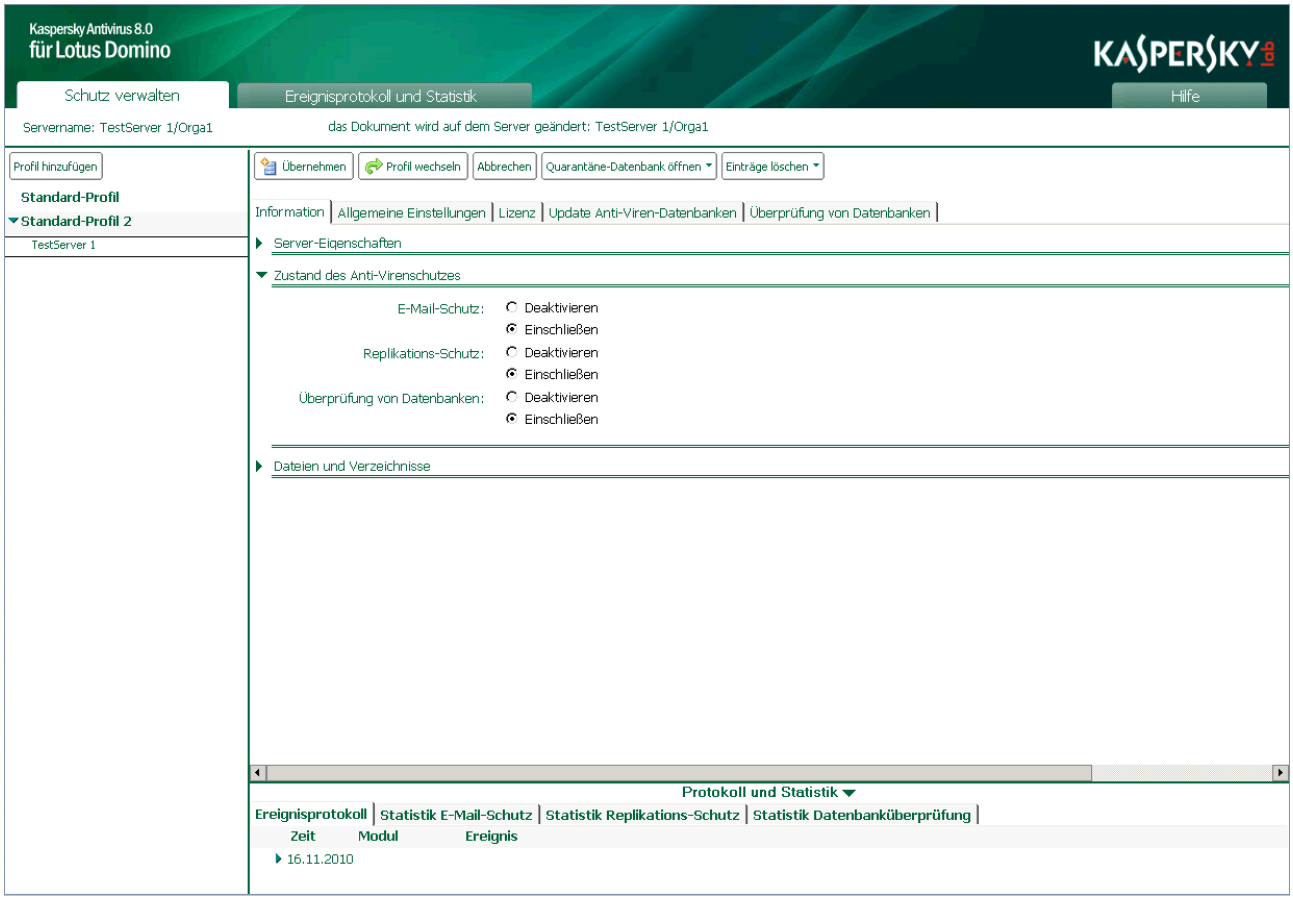


Abbildung 14: E-Mail-Schutz aktivieren / deaktivieren

4. Wählen Sie im Bereich **Zustand des Anti-Virenschutzes** in der Zeile **E-Mail-Schutz** (s. Abbildung oben) und wählen die jeweilige Variante: **Einschließen** oder **Deaktivieren**.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

AUSWAHL VON OBJEKTEN DES E-MAIL-SCHUTZES

Standardmäßig, Wenn der E-Mail-Schutz aktiviert ist, untersucht Kaspersky Anti-Virus standardmäßig den E-Mail-Body, Anhänge aller Formate und eingebettete OLE-Objekte. Wenn nötig, können Sie Untersuchung der aufgezählten Objekte deaktivieren.

Bei der Untersuchung mehrteiliger Archive wird jeder einzelne Archivteil von Kaspersky Anti-Virus als einzelnes Objekt untersucht. Bösartiger Code kann nur dann entdeckt werden, wenn er vollständig in einem der Teile enthalten ist. Falls der Code beispielsweise auf zwei Archivteile verteilt ist, kann er bei der Untersuchung nicht entdeckt werden. Deshalb wird empfohlen, mehrteilige Archive nach dem Speichern auf der Festplatte mit dem Datei Anti-Virus zu untersuchen.

➧ *Um Schutzobjekte zu wählen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die **Ändern** Schaltfläche und im Verwaltungsbereich im **E-Mail-Schutz** Tab wählen Sie **Allgemein** Tab (s. Abbildung unten).

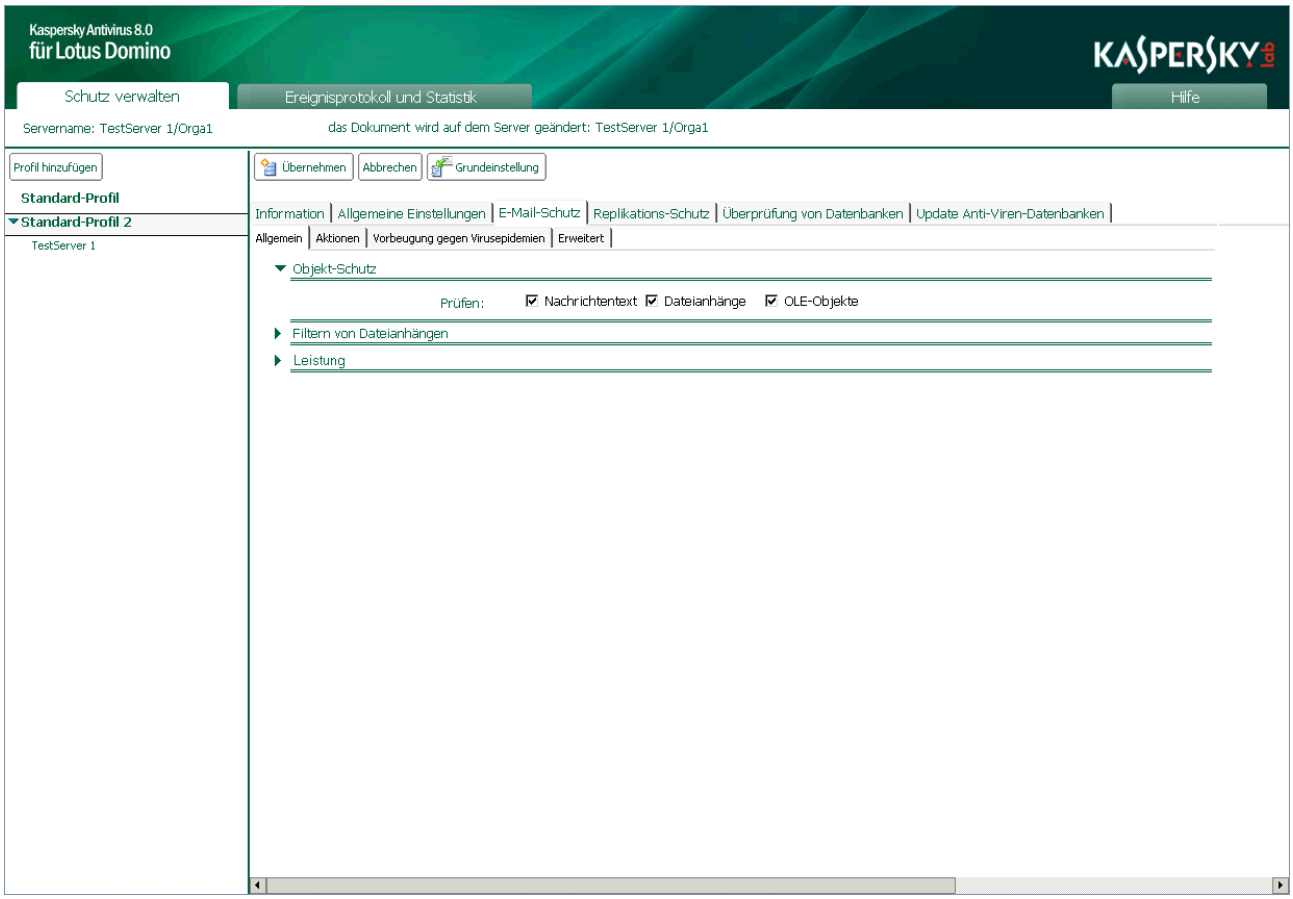


Abbildung 15: Auswahl der Objekte des E-Mail-Schutzes

4. Damit die Objektuntersuchung ausgeführt wird, setzen Sie folgende Häkchen im Bereich **Objekt-Schutz**:

   - **Dateianhänge** – alle E-Mailanhänge untersuchen.
   - **OLE-Objekte** – alle in der E-Mail eingebetteten OLE-Objekte untersuchen.
   - **Nachrichtentext** – den E-Mail-Body untersuchen.

   Wenn das Häkchen nicht gesetzt ist, wird die Untersuchung der entsprechenden Objekte nicht ausgeführt.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

AKTIONEN AN DEN E-MAIL-OBJEKTEN

Kaspersky Anti-Virus verarbeitet Objekte entsprechend dem Status, der den Objekten nach den Ergebnissen der Anti-Viren-Untersuchung und Filterung der Anhänge zugewiesen wurde (s. Abschnitt "Verarbeitung der Objekte und auf sie angewandte Aktionen" auf der S. 25). Nicht infizierte Objekte werden ohne jegliche Änderungen an das E-Mail-System weitergegeben. Nicht infizierte Objekte werden ohne irgendwelche Änderungen übersprungen. Aktionen an desinfizierbaren, nicht desinfizierbaren, möglicherweise infizierten und nicht untersuchten Objekten können vom Administrator konfiguriert werden.

Die Aktionen, welche das Programm ausführen wird, werden separat mit jedem einzelnen Status bestimmt.

- Falls das Objekt als desinfizierbar registriert wurde, wird es von Kaspersky Anti-Virus behandelt und desinfiziert an das E-Mail-System weitergegeben.
- Falls das Objekt als nicht desinfizierbar registriert wurde, wird es von Kaspersky Anti-Virus aus der E-Mail gelöscht.
- Falls das Objekt als möglicherweis infizierte registriert wurde, wird es von Kaspersky Anti-Virus aus der E-Mail gelöscht.
- Falls es nicht gelungen ist, das Objekt zu untersuchen (beispielsweise weil die max. Untersuchungsdauer abgelaufen ist), wird es von Kaspersky Anti-Virus aus der E-Mail gelöscht.

Standardmäßig wird vor der Behandlung oder Löschung eine Objektkopie in der Quarantäne Datenbank gespeichert. Informationen über die entdeckten Objekte und ausgeführten Aktionen werden in die Ereignisprotokoll- und Statistikdatenbanken eingetragen (s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98).

Nach Virenprüfung aller Objekte einer E-Mail und Ausführung aller geforderten Aktionen, kann eine der folgenden weiteren Aktionen für die gesamten E-Mail ausgeführt werden:

- Zusätzliche Information zum Betreff oder E-Mail-Body hinzufügen;
- Benachrichtigungen zusammenstellen und an den Absender/Empfänger und den Administratoren ausliefern (standardmäßig deaktiviert);
- Eine Kopie der gesamten Ausgangsmail in die Quarantäne Datenbank verschieben (standardmäßig deaktiviert).

Um Aktionen für Objekte zu konfigurieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Betätigen Sie im Action panel die **Ändern** Schaltfläche und im Verwaltungsbereich im Tab **E-Mail-Schutz** wählen Sie den **Aktionen** Tab (s. Abbildung unten).

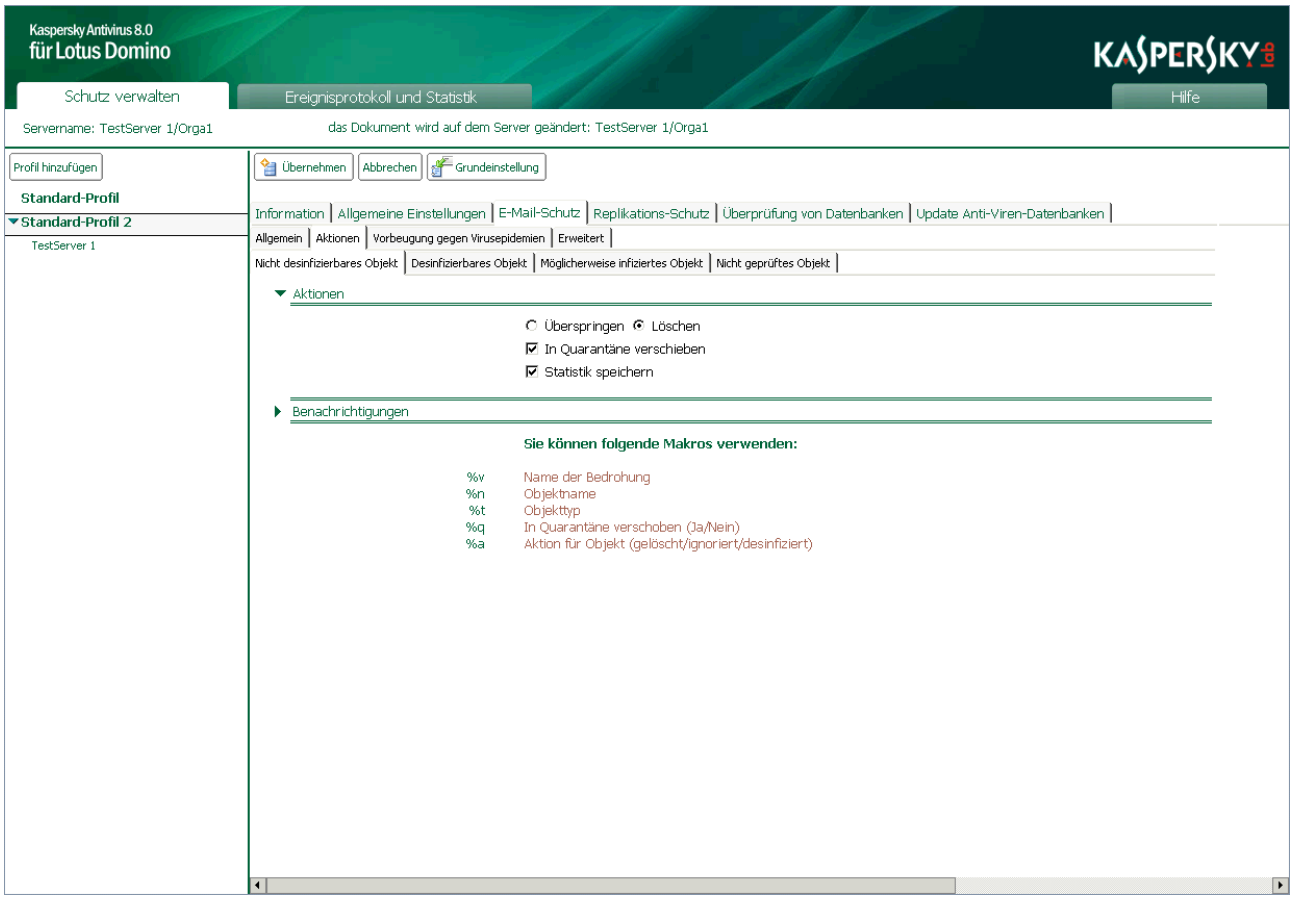


Abbildung 16: Einstellung von Aktionen an nicht desinfizierbaren Objekten im E-Mail-Schutz Modus

4. Unter dem **Aktionen** Tab wählen Sie den Tab, der dem Status des Objekts, dessen Verarbeitung Sie anpassen wollen, entspricht. Sie können aus folgenden Tabs wählen

   - **Nicht desinfizierbares Objekt** – Anpassung der Verarbeitungseinstellungen von unheilbaren Objekten.
   - **Desinfizierbares Objekt** – Einstellungsanpassung für die Verarbeitung desinfizierbarer Objekte.
   - **Möglicherweise infiziertes Objekt** – Einstellungsanpassung für die Verarbeitung möglicherweise infizierter Objekte.
   - **Nicht geprüftes Obj**ekt – Einstellungsanpassung für die Verarbeitung nicht untersuchter Objekte.

5. Im **Aktionen** Bereich (s. Abbildung oben) wählen Sie die Aktion, die an einem entdeckten Objekt ausgeführt werden soll. Setzen Sie zu folgende Häkchen:

   - **In Quarantäne verschieben** – vor der Verarbeitung wird eine Objektkopie in der Quarantäne Datenbank gespeichert.

   Falls in den Schutzparametern im Tab **Erweitert**, das Häkchen bei **Ganze Nachricht in Quarantäne verschieben** gesetzt ist, werden einzelne Objekte nicht gespeichert. Nach der Untersuchung aller Bestandteile der E-Mail wird eine Kopie der Ausgangsmail mit allen Anhängen in der Quarantäne Datenbank gespeichert. Falls das Häkchen bei **Ganze Nachricht in Quarantäne verschieben** nicht gesetzt ist, wird nur das Objekt verschoben, die E-Mail wird nicht in die Quarantäne verschoben.

- **Statistik speichern** – Information über entdeckte Objekte und ausgeführte Aktionen werden an den Orten,welche im Feld **Information speichern**, im Tab **Allgemeine Einstellungen** angegeben sind, gespeichert. Falls mehrere Orte gleichzeitig zur Informationsaufbewahrung ausgewählt werden, wird die Information an den angegebenen Orten der Informationsaufbewahrung auch gleichzeitig eingetragen.

  - **In die Konsole** (Systemprotokoll Domino log.nsf);
  - **Ins Protokoll**;
  - **In Datei** (standardmäßiger Dateiname server.log_N, wobei N — Ordnungsnummer der Log-Datei ist).

6. Im **Benachrichtigungen** Bereich (s. Abbildung unten) passen Sie die Einstellungen an, aufgrund welcher die Benachrichtigungen über entdeckte Objekte und ausgeführte Aktionen geschrieben werden (s. Abschnitt "Benachrichtigungen" auf der S. 109).

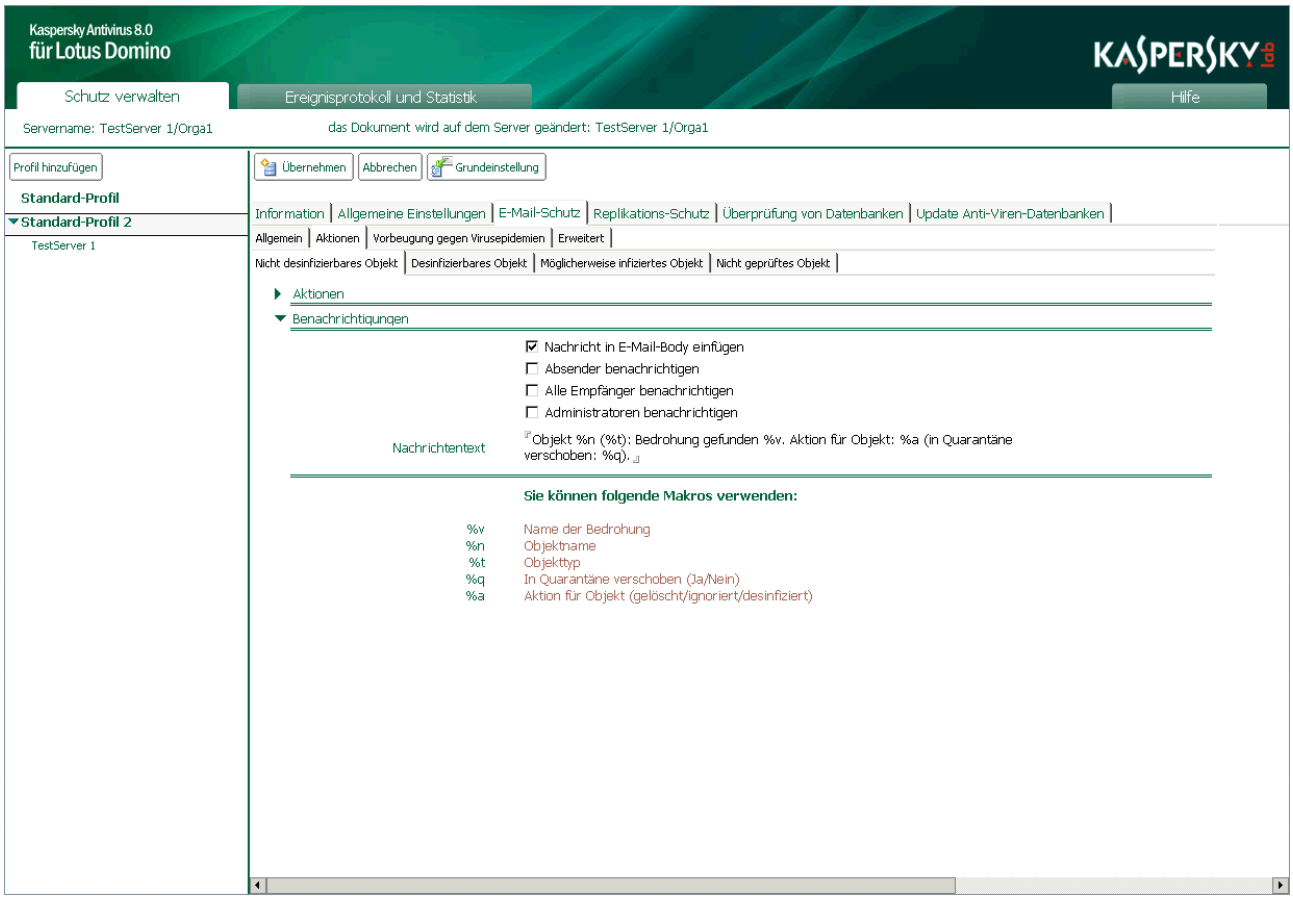


Abbildung 17: Anpassung der Einstellungen der der Benachrichtigungen

7. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

➧ *Um die Aktionen festzulegen, welche nach der Untersuchung der E-Mails und deren ausgeführt werden, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im **Replikations-Schutz** Tab wählen Sie den Tab **Erweitert** (s. Abbildung unten).

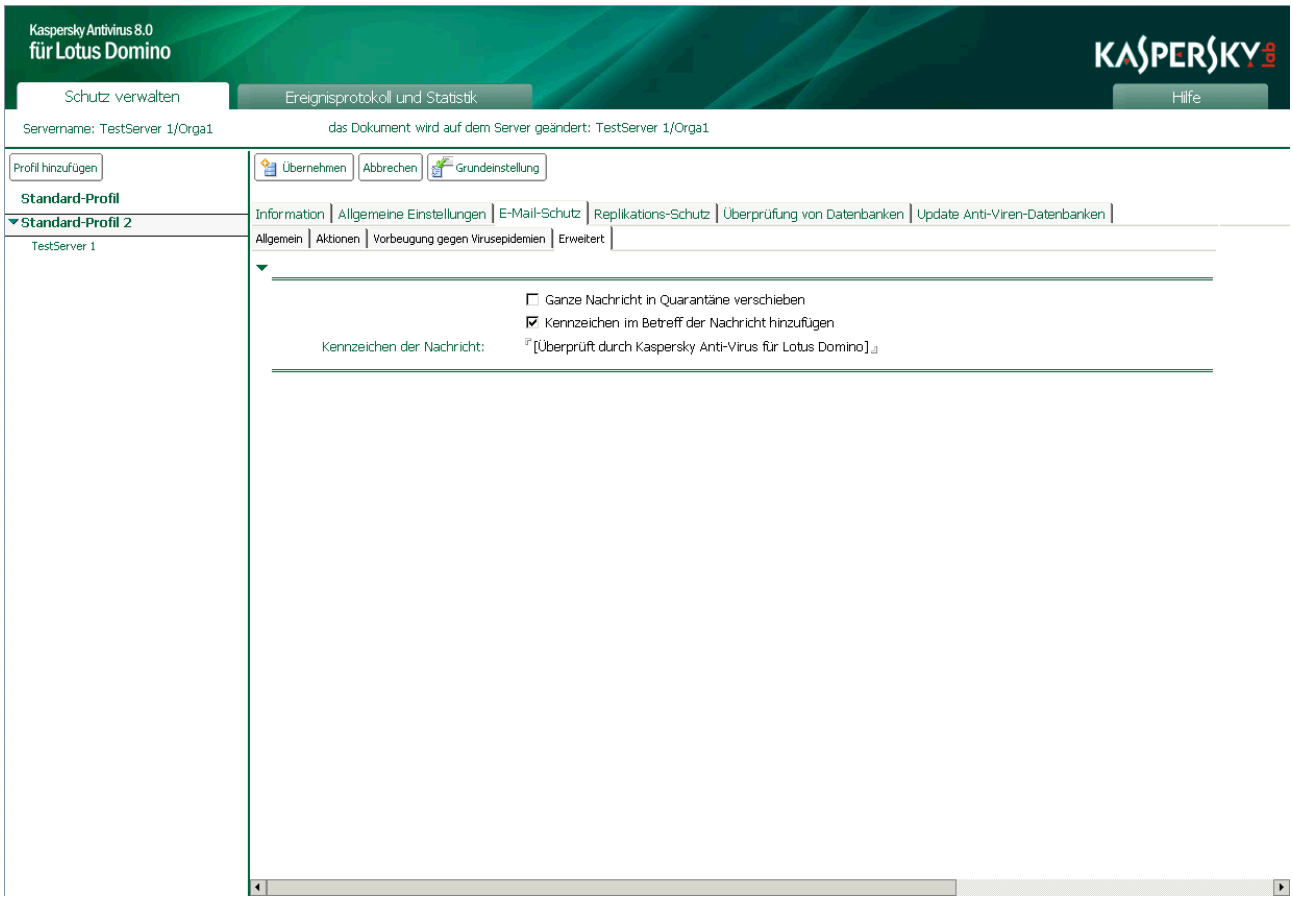


Abbildung 18: Anpassung der Aktionen nach der E-Mailüberprüfung

4. Im **Erweitert** Tab führen Sie folgende Aktionen aus:

   - Setzen Sie das Häkchen bei **Ganze Nachricht in Quarantäne verschieben**. Als Folge wird nach der Untersuchung eine Kopie aller zur E-Mail gehörenden Objekte in der Quarantäne Datenbank gespeichert.

   - Setzen Sie das **Kennzeichen im Betreff der Nachricht hinzufügen** Häkchen und im Bereich **Kennzeichen der Nachricht** erstellen Sie den Text, der zum Betreff der untersuchten E-Mail hinzugefügt wird. Standardmäßig enthält der Bereich **Kennzeichen der Nachricht** folgende Angabe **Überprüft durch Kaspersky Antivirus für Lotus Domino**.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

FILTERN VON E-MAIL-ANHÄNGEN

Kaspersky Anti-Virus kann E-Mail-Anhänge ausfiltern (s. Abschnitt "Algorithmus zur Filterung von Anhängen" auf der S. 24). Mittels Filterung können Sie, den Filtereinstellungen entsprechende Anhänge aus der Anti-Viren-Untersuchung ausschließen und eine besondere Verarbeitung für diese vorgeben. Standardmäßig wird im E-Mail-Schutz Modus keine Anhangsfilterung durchgeführt.

Um die Anhangsfilterung zu konfigurieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im **E-Mail-Schutz** Tab wählen Sie den Tab **Erweitert** (s. Abbildung unten).

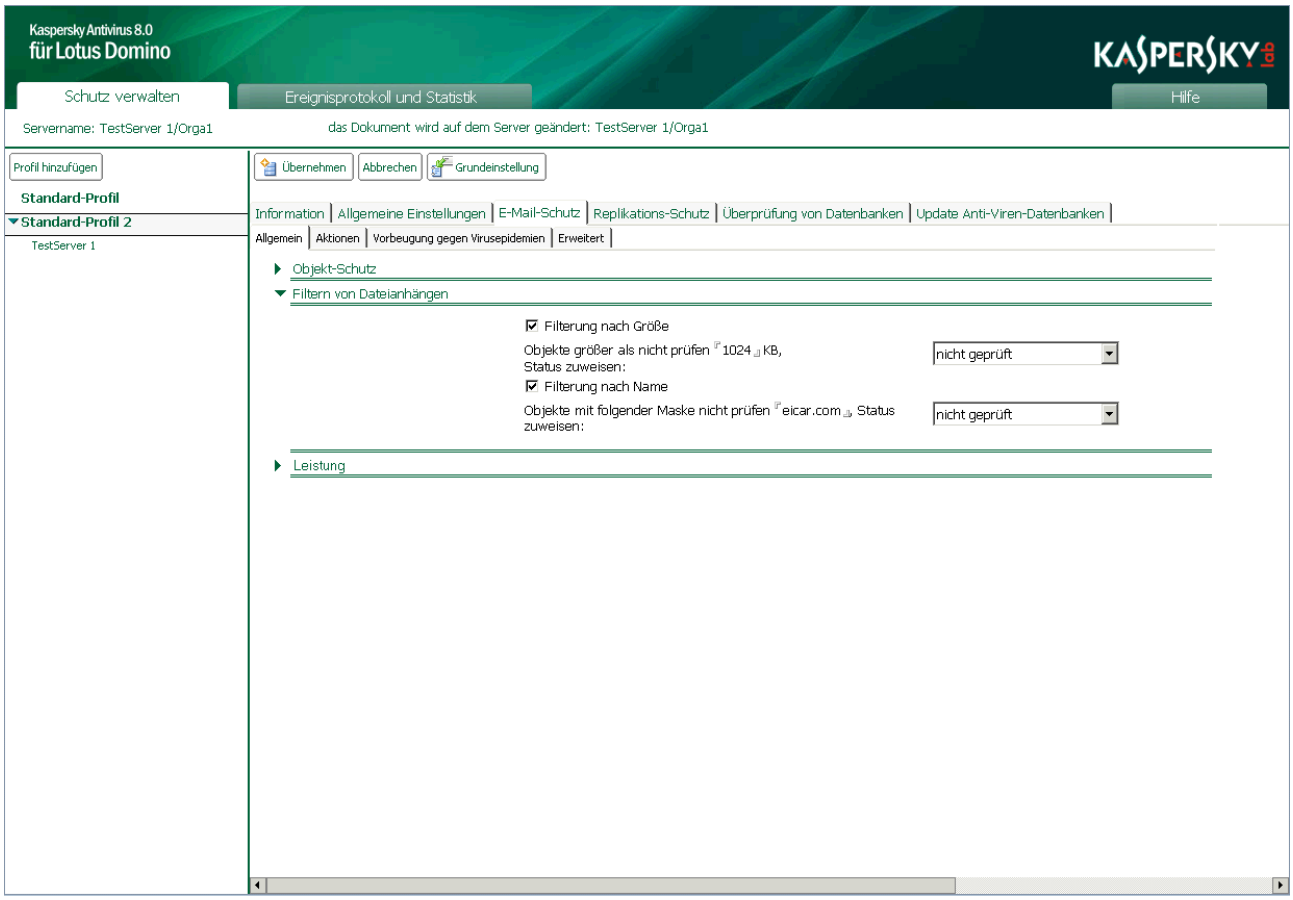


Abbildung 19: Anpassen der Anhangs-Filtereinstellungen

4. Damit die **Filterung der Anhänge** durchgeführt wird, setzen Sie folgende Häkchen im Bereich Filtern von Dateianhängen :

   - **Filterung nach Größe**. Setzen Sie dieses Häkchen, damit Kaspersky Anti-Virus die Größe der Anhänge untersucht. Im **Objekte größer als nicht prüfen** Feld geben Sie den Wert in Kilobyte (KB) ein. Bei einer Überschreitung wird das Objekt ausgefiltert und von der Anti-Viren-Untersuchung ausgeschlossen. Aus der geöffneten Liste wählen Sie den Status, dementsprechend das Objekt von Kaspersky Anti-Virus verarbeitet werden soll. Standardmäßig ist der Status *nicht geprüft* gewählt.

   - **Filterung nach Name**. Setzen Sie dieses Häkchen, damit Kaspersky Anti-Virus die Namen der Anhänge untersucht. Im **Objekte mit folgender Maske nicht prüfen** Feld geben Sie die Dateiennamensmasken an,

anhand welcher ausgefiltert und von der Anti-Viren-Untersuchung ausgeschlossen wird. Aus der geöffneten Liste wählen Sie den Status, dementsprechend das Objekt von Kaspersky Anti-Virus verarbeitet werden soll. Standardmäßig ist der Status *nicht geprüft* gewählt.

Beim Filtern nach Namen wird nach Groß- und Kleinschreibung unterschieden.

Sie können mehrere durch";" Zeichen voneinander getrennten Masken angeben. Bei der Maskenerstellung verwenden Sie folgende Zeichen:

- * – jegliche Reihenfolge von Zeichen. Zum Beispiel,wird bei Angabe dieser abc*-Maske wird keine Datei, deren Name mit der Zeichenfolge abc beginnt, untersucht: abc.exe, abc1.com, abc2.rar.
- ? – beliebiges Zeichen. Beispielsweise wird bei Angabe dieser abc?.exe-Maske jede Datei, deren Name mit der Zeichenfolge abc beginnt und mit einem beliebigen Zeichen, das nach c folgt, ergänzt wird, nicht untersucht. Z.B. abc1.exe.

Falls das Häkchen nicht gesetzt ist, wird die Filterung entsprechender Objekte nicht durchgeführt.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

BENACHRICHTIGUNGEN ÜBER EPIDEMIEN

Kaspersky Anti-Virus meldet den Administratoren den Anstieg an infizierten, möglicherweise infizierten und beschädigten Objekten, die bei der Untersuchung der E-Mails entdeckt wurden, sowie die Menge von Objekten, die eine gleichartige Bedrohung enthalten.

Für jede der aufgezählten Kategorien stellt Kaspersky Anti-Virus die Menge von Objekten, die im vorgegebenen Zeitraum entdeckt wurden, fest. Bei einer Überschreitung des maximal zulässigen Wertes meldet Anti-Virus dies den Server- und Profiladministratoren und schreibt entsprechende Einträge in das Ereignisprotokoll.

Diese Option kann auch bei Virenepidemien behilflich sein und ermöglicht es, auf auftretende Virenangriffe rechtzeitig zu reagieren.

Serveradministratoren werden in den Servereinstellungen angegeben (s. Abschnitt "Einsetzung vom Serveradministrator" auf der S. 114): Im Tab **Information** im Bereich **Server-Eigenschaften**. Die Profiladministratoren werden in den Profileinstellungen angegeben (s. Abschnitt "Einsetzung vom Profiladministrator" auf der S. 114): Im Tab **Allgemeine Einstellungen** im Bereich **Sicherheit**.

Die Benachrichtigungseinstellungen über aufkommende Bedrohungen zur Entstehung einer Epidemie, werden in den E-Mail-Schutz Einstellungen für jede Objektkategorie separat angegeben.

➧ *Um die Benachrichtigungseinstellungen bei Epidemien anzupassen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im **E-Mail-Schutz** Tab wählen Sie den Tab **Vorbeugung gegen Virusepidemien** (s. Abbildung unten).

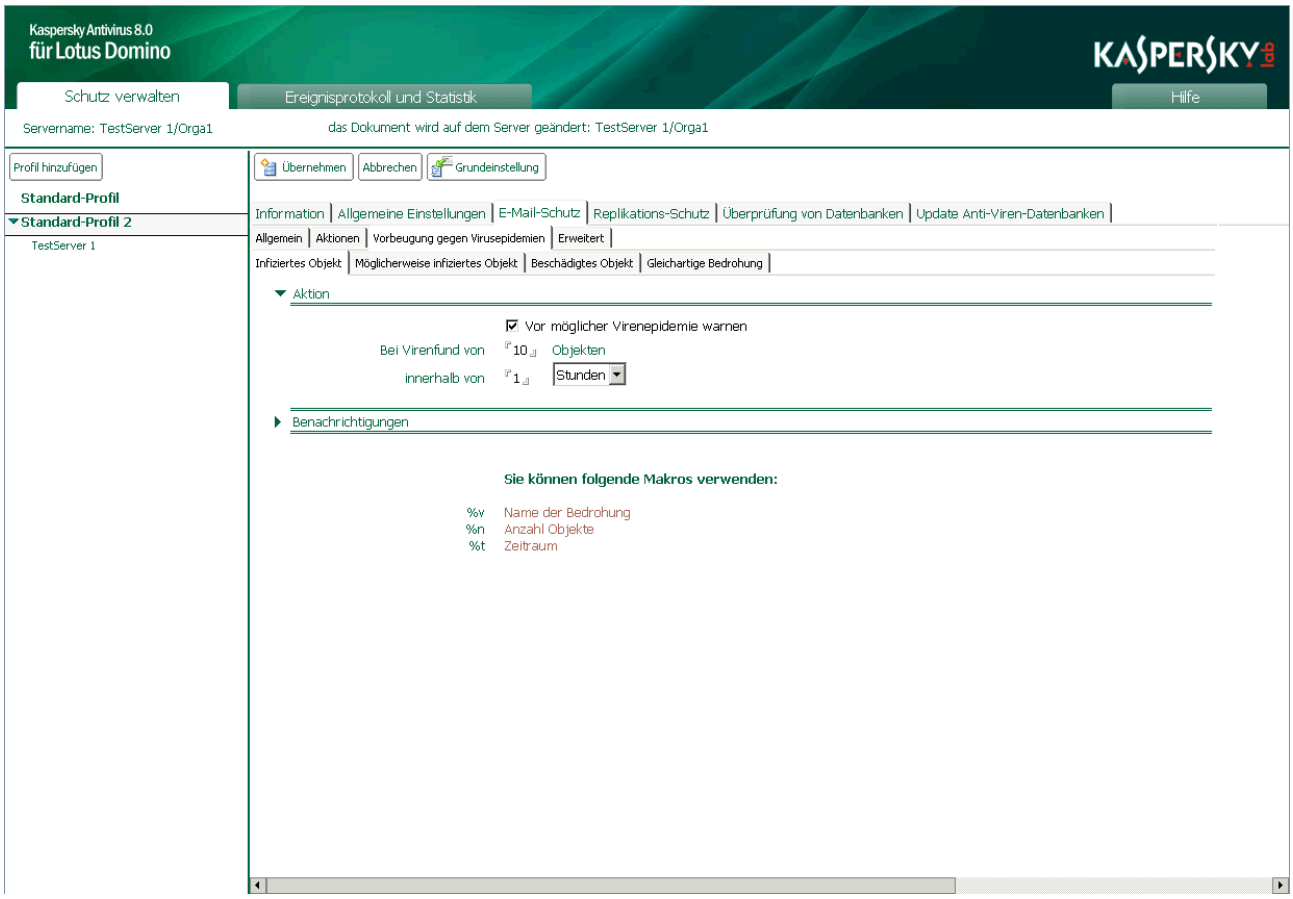


Abbildung 20: Anpassung der Einstellungen über Benachrichtigungen bei Epidemien

4. Im Tab **Vorbeugung gegen Virusepidemien,** wählen Sie den Tab, der den Objektkategorien, für die Sie die Einstellungen der Benachrichtigungen über Epidemien anpassen wollen, entspricht. Sie können aus folgenden Tabs wählen

   - **Infiziertes Objekt** – Einstellungsanpassungd er Benachrichtigungen über eine Überschreitung der maximalen zulässigen Menge von entdeckten infizierten Objekten (desinfizierbar und nicht desinfizierbar insgesamt).

   - **Möglicherweise infiziertes Objekt** – Einstellungsanpassung der Benachrichtigungen über eine Überschreitung der maximalen zulässigen Menge von entdeckten möglicherweise infizierten Objekten.

   - **Beschädigtes Objekt** – Einstellungsanpassungd er Benachrichtigungen über eine Überschreitung der maximalen zulässigen Menge von entdeckten nicht untersuchten Objekten.

   - **Gleichartige Bedrohung** – Einstellungsanpassung der Benachrichtigungen über eine Überschreitung der maximalen zulässigen Menge von Objekten, in denen eine gleichartige Bedrohung entdeckt wurde.

5. Im **Aktion** Bereich (s. Abbildung oben) setzen Sie das Häkchen bei **Vor möglicher Virenepidemie warnen**, um den Mechanismus zur Verhinderung von Epidemien zu aktivieren. Weiterhin geben Sie die Einstellungswerte an, aufgrund welcher die Benachrichtigung versendet werden: Die maximal zulässige Objektmenge und den Zeitraum, während dessen diese entdeckt werden müssen.

6. Im Bereich **Benachrichtigungen** (s. Abbildung unten) im **Nachrichtentext** Feld erstellen Sie den Text der Benachrichtigungsmeldung, welcher via E-Mail an die Administratoren-Adresse gesendet wird. Sie können folgende Makros verwenden:

   - **%v** – Name der im Objekt entdeckten Bedrohung;

- **%n** – Objektmenge;
- **%t** – Zeitraum, während dessen die Objekte entdeckt wurden.

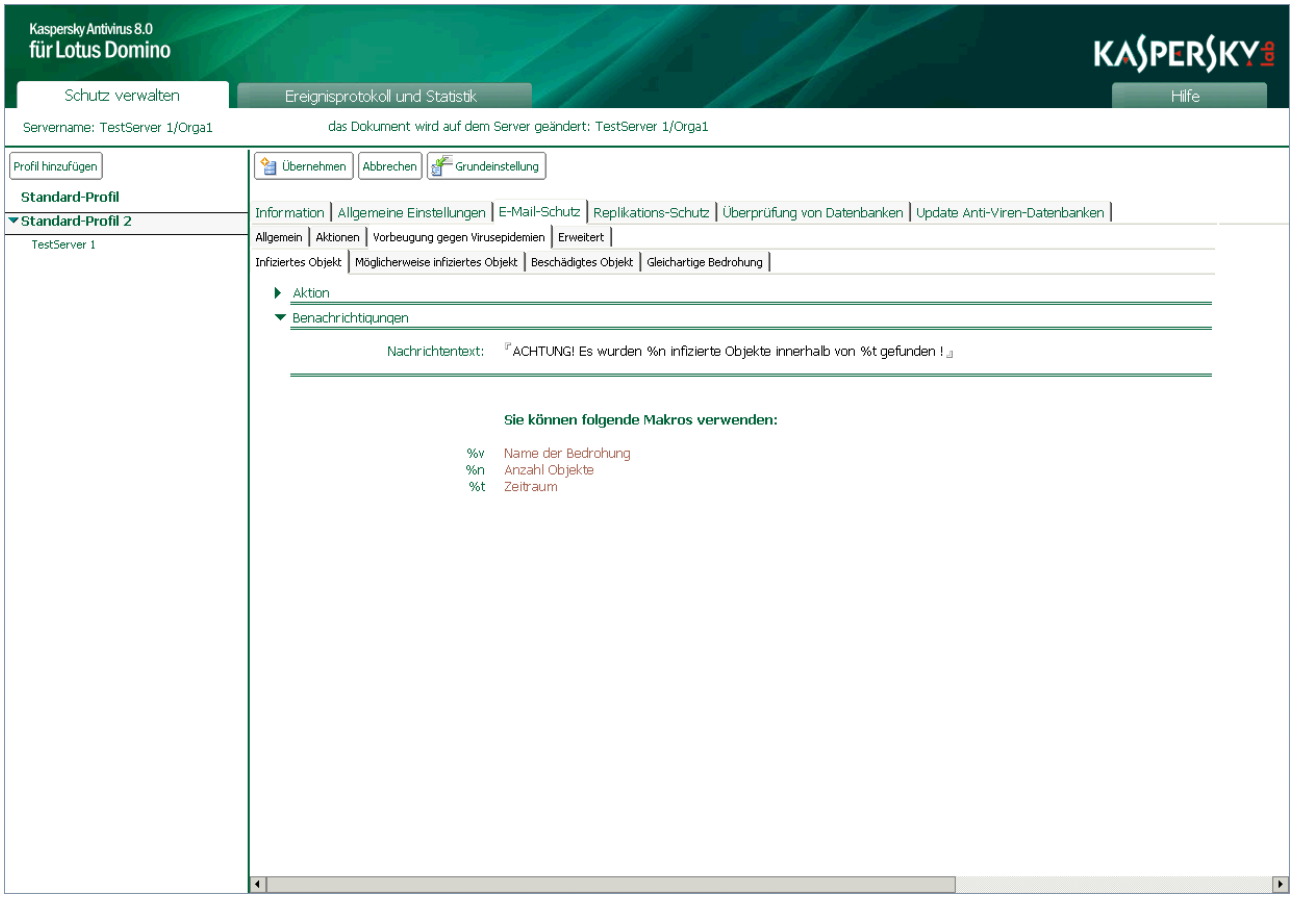


Abbildung 21: Erstellung des Benachrichtigungstextes

7. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

REPLIKATIONSSCHUTZ

Wenn der Anti-Viren-Replikationsschutz aktiviert ist (s. Abschnitt "Replikationsschutz aktivieren / deaktivieren" auf der S. 72), untersucht Kaspersky Anti-Virus die auf dem geschützten Server gespeicherten Dokumente, die während einer Replikation geändert wurden. Auf Bedrohungen untersucht werden der Inhalt von RTF-Feldern in Dokumenten, Anhänge von Dokumenten und eingebettete OLE-Objekte. Ausgehende Replikationen werden nicht untersucht.

Die bei der Untersuchung entdeckten infizierten, möglicherweise infizierten und wegen einer Störung oder Beschädigung nicht untersuchten Objekte werden gemäß den Replikationsschutz-Einstellungen verarbeitet (s. Abschnitt "Aktionen für Objekte im Modus des Replikationsschutzes" auf der S. 74).

Nach der Programminstallation werden Standardeinstellungen verwendet (s. Abschnitt "Standardmäßiger Serverschutz" auf der S. 49). Sie können sie den gestellten Sicherheitsanforderungen entsprechend anpassen. Ein Teil dieser aufgezählten Einstellungen ist standardmäßig deaktiviert oder kann von einem Administrator deaktiviert werden.

Für Anhänge, deren Größe den vorgegebenen Wert überschreitet und / oder deren Namen der angegebenen Dateinamensmaske entsprechen, kann eine gesonderte Verarbeitung eingestellt werden (s. Abschnitt "Filtern von Anhängen im Modus des Replikationsschutzes" auf der S. 76).

Standardmäßig wird vor der Verarbeitung eine Kopie des Objekts in die Quarantäne verschoben (s. Abschnitt "Quarantäne" auf der S. 91). Ein Dokument, welches das Objekt beherbergt, wird nicht in Quarantäne verschoben.

Es werden Benachrichtigung über die Überprüfung eines Dokumentes, welches durch Kaspersky Anti-Virus untersucht wurde und die Beschreibung der ausgeführten Aktionen, an die Administratoren gesendet (s. Abschnitt "Benachrichtigungen" auf der S. 109). Informationen über die Untersuchungsergebnisse und ausgeführten Aktionen werden in die Ereignisprotokoll- und Statistikdatenbanken eingetragen (s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98).

Wenn nötig, können Sie die Untersuchung von Anhängen, OLE-Objekten und Inhalte von Feldinhalten deaktivieren (s. Abschnitt "Auswahl von Objekten des Replikationsschutzes" auf der S. 73). Sie können auch die Untersuchungsdauer einzelner Objekte beschränken, was die gesamte Performance der E-Mailuntersuchung wesentlich steigert (s. Abschnitt "Leistung" auf der S. 89).

Dabei können Objekte, deren Größe den vorgegebenen Wert nicht überschreiten, im Arbeitsspeicher des Servers, ohne auf der Festplatte gespeichert zu werden, untersucht werden (s. Abschnitt "Leistung" auf der S. 89).

Die Einstellungen des Replikationsschutzes werden von dem Profil vorgegeben, welches den geschützten Server einschließt. Die Anpassung einzelner Einstellungen des Replikationsschutzes für einen Server ist nicht vorgesehen. Allerdings kann der Replikationsschutz nur für jeden einzelnen Server separat aktiviert (deaktiviert) werden (s. Abschnitt "Replikationsschutz aktivieren / deaktivieren" auf der S. 72).

IN DIESEM ABSCHNITT

Replikationsschutz aktivieren / deaktivieren 72

Auswahl von Objekten des Replikationsschutzes 73

Aktionen für Objekte im Modus des Replikationsschutzes 74

Filtern von Anhängen im Modus des Replikationsschutzes 76

REPLIKATIONSSCHUTZ AKTIVIEREN / DEAKTIVIEREN

Standardmäßig ist der Replikationsschutz aktiviert und wird beim Hochfahren des Domino-Servers automatisch gestartet. Informationen über den Start der Module, welche den Replikationsschutz sichern, werden in das Kaspersky Anti-Virus Ereignisprotokoll geschrieben.

Wenn nötig, können Sie den Replikationsschutz aktivieren und deaktivieren. Entsprechende Operationen werden für jeden einzelnen Server separat durchgeführt.

Um den Replikationsschutz zu aktivieren / deaktivieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie den Server aus dem Profilbestand, für welchen Sie den Replikationsschutz deaktivieren wollen.

3. Im Action panel betätigen Sie die **Ändern** Schaltfläche und im Verwaltungsbereich wählen Sie den **Information** Tab (s. Abbildung unten).

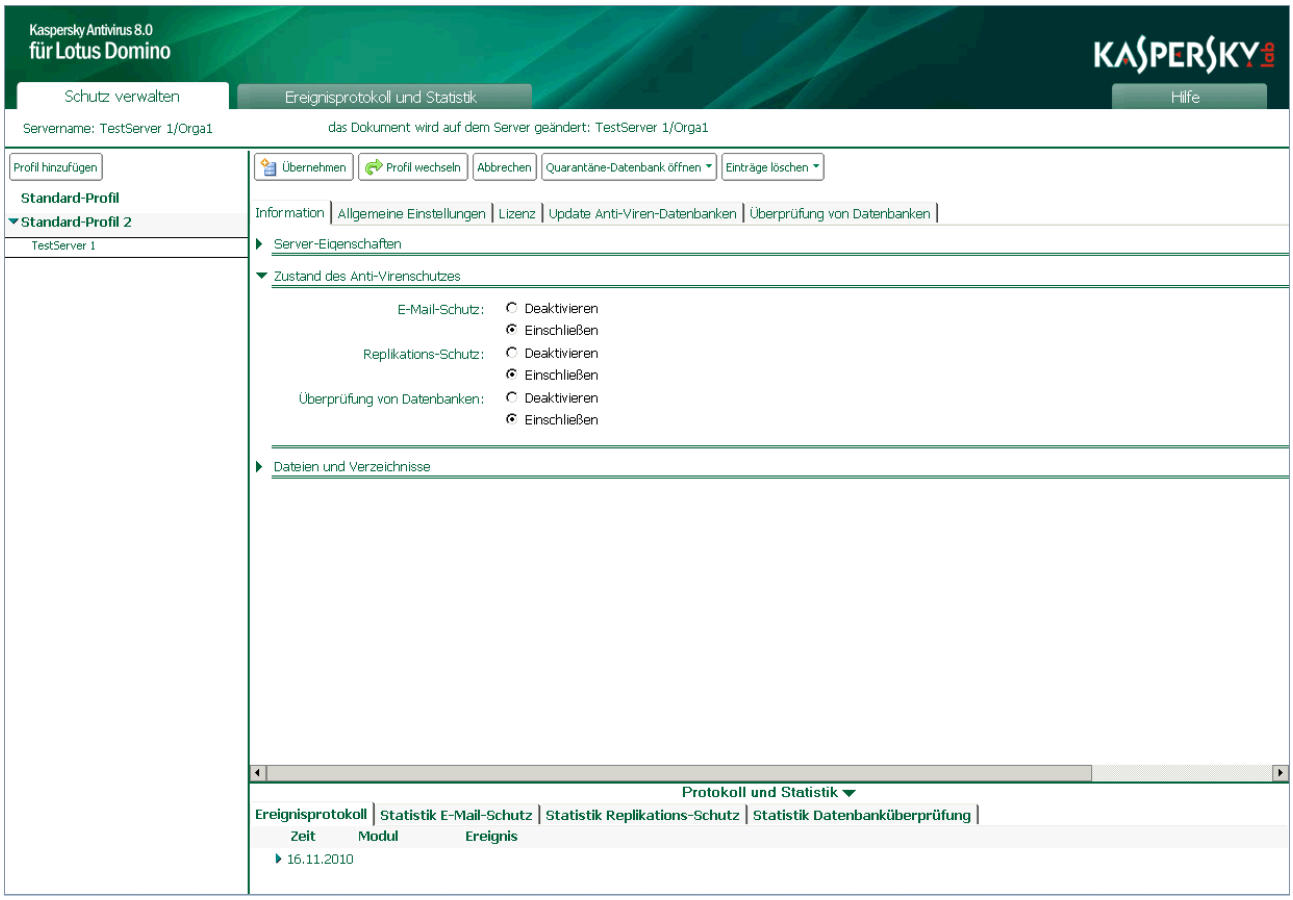


Abbildung 22: Replikationsschutz aktivieren / deaktivieren

4. Wählen Sie im Bereich **Zustand des Anti-Virenschutzes** in der Zeile **Replikations-Schutz** (s. Abbildung oben) und wählen die jeweilige Variante: **Einschließen** oder **Deaktivieren**.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

AUSWAHL VON OBJEKTEN DES REPLIKATIONSSCHUTZES

Wenn der Anti-Viren-Replikationsschutz aktiviert ist, untersucht Kaspersky Anti-Virus standardmäßig den Inhalt von Feldern, Anhänge aller Formate und eingebettete OLE-Objekte in RTF-Dokumenten. Wenn nötig, können Sie Untersuchung der aufgezählten Objekte deaktivieren.

Bei der Untersuchung mehrteiliger Archive wird jeder einzelne Archivteil von Kaspersky Anti-Virus als einzelnes Objekt untersucht. Bösartiger Code kann nur dann entdeckt werden, wenn er vollständig in einem der Teile enthalten ist. Falls der Code beispielsweise auf zwei Archivteile verteilt ist, kann er bei der Untersuchung nicht entdeckt werden. Deshalb wird empfohlen, mehrteilige Archive nach dem Speichern auf der Festplatte mit dem Datei Anti-Virus zu untersuchen.

Um Schutzobjekte zu wählen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.
3. Im Action panel betätigen Sie die **Ändern** Schaltfläche und im Verwaltungsbereich im Tab **Replikations-Schutz** wählen Sie den Tab **Allgemein** (s. Abbildung unten).

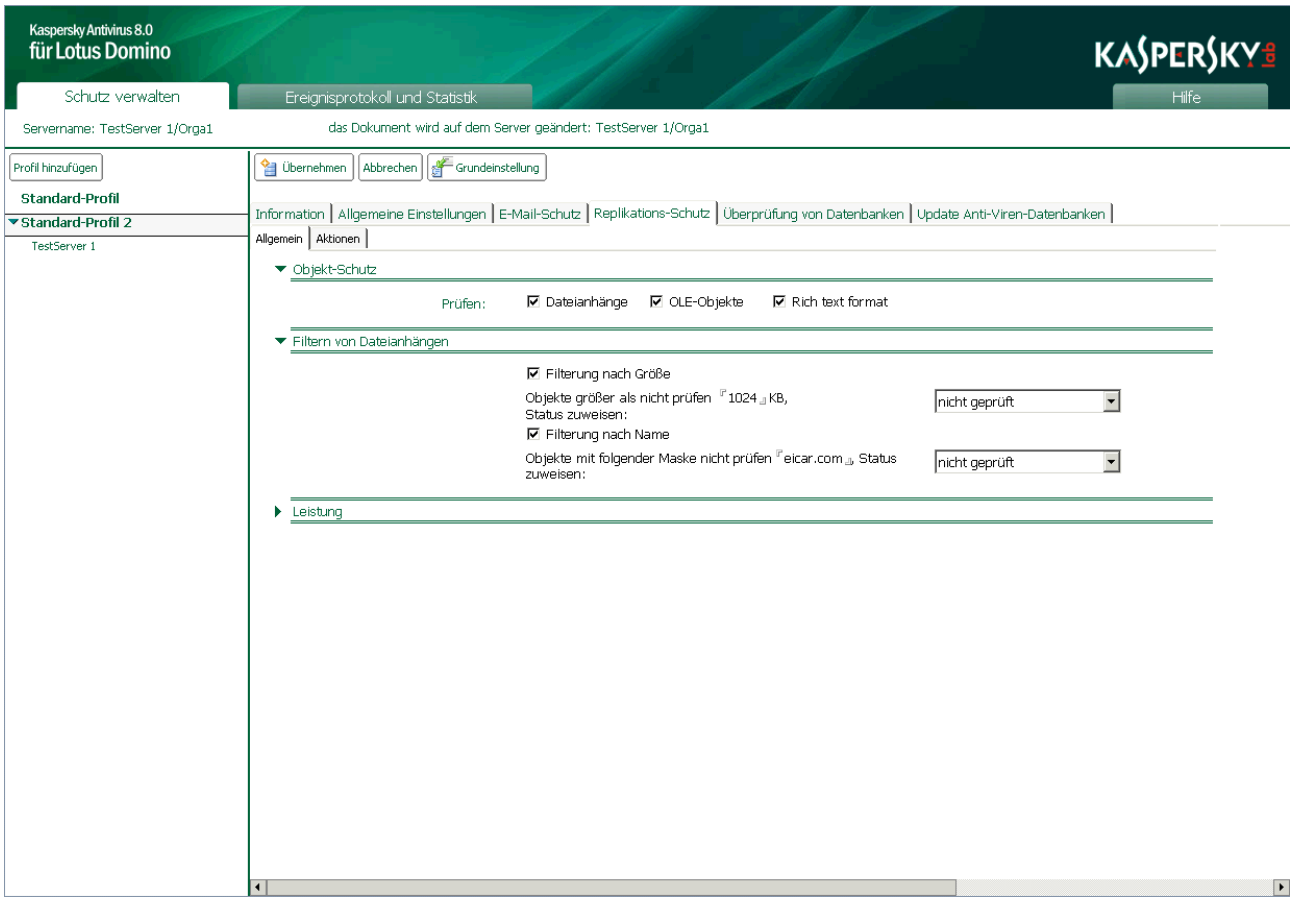


Abbildung 23: Auswahl der Objekte des Replikationsschutzes

4. Damit die Objektuntersuchung ausgeführt wird, setzen Sie folgende Häkchen im Bereich **Objekt-Schutz** :
   - **Dateianhänge** – alle Dokumentanhänge untersuchen.
   - **OLE-Objekte** – alle in der Meldung eingebetteten OLE-Objekte untersuchen.
   - **Rich text format** – Felder des Dokuments im Rich Text Format untersuchen.

Wenn das Häkchen nicht gesetzt ist, wird die Untersuchung der entsprechenden Objekte nicht ausgeführt.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

AKTIONEN FÜR OBJEKTE IM MODUS DES REPLIKATIONSSCHUTZES

Kaspersky Anti-Virus verarbeitet Objekte entsprechend dem Status, der den Objekten nach den Ergebnissen der Anti-Viren-Untersuchung und Filterung der Anhänge zugewiesen wurde (s. Abschnitt "Verarbeitung der Objekte und auf sie angewandte Aktionen" auf der S. 25). Nicht infizierte Objekte werden im Dokument ohne irgendwelche Änderungen festgehalten. Nicht infizierte Objekte werden ohne irgendwelche Änderungen übersprungen. Aktionen an desinfizierbaren, nicht desinfizierbaren, möglicherweise infizierten und nicht untersuchten Objekten können vom Administrator konfiguriert werden.

Die Aktionen, welche das Programm ausführen wird, werden separat mit jedem einzelnen Status bestimmt.

- Es werden folgende standardmäßige Aktionen an den Objekten ausgeführt.
- Falls das Objekt als nicht desinfizierbar registriert wurde, wird es von Kaspersky Anti-Virus aus dem Dokument gelöscht.
- Falls das Objekt als möglicherweise infiziertes registriert wurde, wird es von Kaspersky Anti-Virus aus dem Dokument gelöscht.
- Falls es nicht gelungen ist, das Objekt zu untersuchen (beispielsweise, weil die Untersuchungsdauer überschritten wurde), wird es von Kaspersky Anti-Virus aus der Meldung gelöscht.

Standardmäßig wird vor der Behandlung oder Löschung eine Objektkopie in der Quarantäne Datenbank gespeichert. Informationen über entdeckte Objekte und ausgeführte Aktionen können an die Administratoren gesendet werden (s. Abschnitt "Benachrichtigungen" auf der S. 109) und in der Ereignisprotokoll- und Statistikdatenbank gespeichert werden(s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98).

➧ *Um die Einstellungen der Objektverarbeitung anzupassen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im **E-Mail-Schutz** Tab wählen Sie den Tab **Erweitert** (s. Abbildung unten).

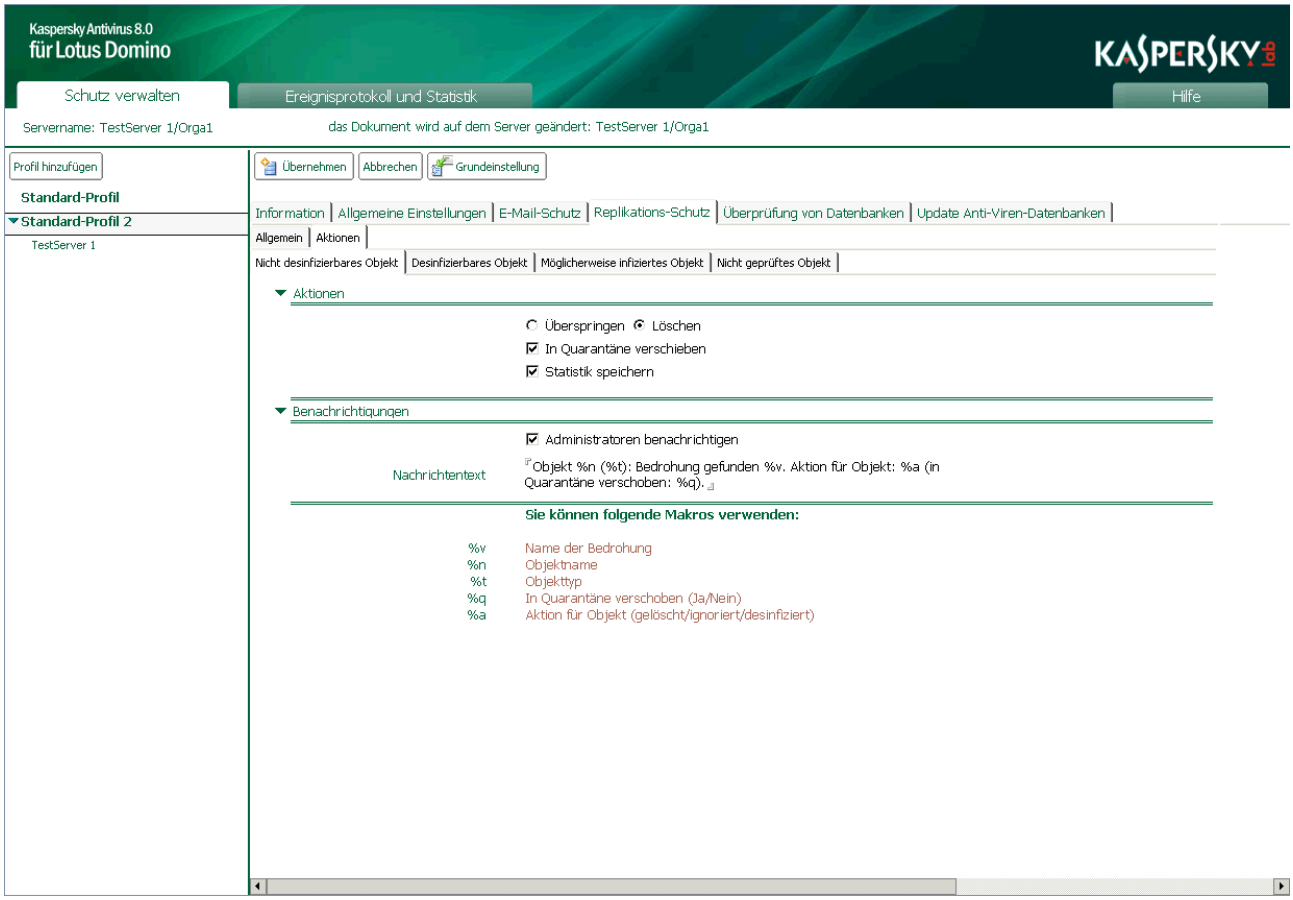


Abbildung 24: Anpassung der Aktionen an nicht desinfizierbaren Objekten im Modus des Replikationsschutzes

4. Im **Aktionen** Tab wählen Sie den Tab, der dem Status des Objekts entspricht, dessen Verarbeitungseinstellungen Sie anpassen möchten. Sie können aus folgenden Tabs wählen

   - **Nicht desinfizierbares Objekt** – Anpassung der Verarbeitungseinstellungen von unheilbaren Objekten.
   - **Desinfizierbares Objekt** – Anpassung der Verarbeitungseinstellungen von desinfizierbaren Objekten.
   - **Möglicherweise infiziertes Objekt** – Anpassung der Verarbeitungseinstellungen von möglicherweise infizierten Objekten.
   - **Nicht geprüftes Objekt** – Anpassung der Verarbeitungseinstellungen von nicht untersuchten Objekten.

5. Im **Aktionen** Bereich (s. Abbildung oben) wählen Sie die Aktion, die an einem entdeckten Objekt ausgeführt werden soll. Setzen Sie zu folgende Häkchen:

   - **In Quarantäne verschieben** – vor der Verarbeitung wird eine Objektkopie in der Quarantäne Datenbank gespeichert.

     In Quarantäne wird nur das Objekt selbst verschoben. Ein Dokument, welches das Objekt beherbergt, wird nicht in Quarantäne verschoben.

   - **Statistik speichern** – Information über entdeckte Objekte und ausgeführte Aktionen werden an den Orten,welche im Feld **Information speichern**, im Tab **Allgemeine Einstellungen** angegeben sind, gespeichert. Falls mehrere Orte gleichzeitig zur Informationsaufbewahrung ausgewählt werden, wird die Information an den angegebenen Orten der Informationsaufbewahrung auch gleichzeitig eingetragen.

- **In die Konsole** (Systemprotokoll Domino log.nsf);
- **Ins Protokoll**;
- **In Datei** (Dateiname auf Grundeinstellung server.log).

6. Im **Benachrichtigungen** Bereich (s. Abbildung unten) passen Sie die Einstellungen an, aufgrund welcher die Benachrichtigungen über entdeckte Objekte und ausgeführte Aktionen geschrieben werden (s. Abschnitt "Benachrichtigungen" auf der S. 109).

7. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

FILTERN VON ANHÄNGEN IM MODUS DES REPLIKATIONSSCHUTZES

Kaspersky Anti-Virus kann Dokumentenanhänge ausfiltern (s. Abschnitt "Algorithmus zur Filterung von Anhängen" auf der S. 24). Mittels Filterung können Sie, den Filtereinstellungen entsprechende Anhänge aus der Anti-Viren-Untersuchung ausschließen und eine besondere Verarbeitung für diese vorgeben. Standardmäßig wird im Replikationsschutz-Modus keine Filterung von Anhängen durchgeführt.

Um die Anhangsfilterung zu konfigurieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im **Replikations-Schutz** Tab wählen Sie den Tab **Erweitert** (s. Abbildung unten).

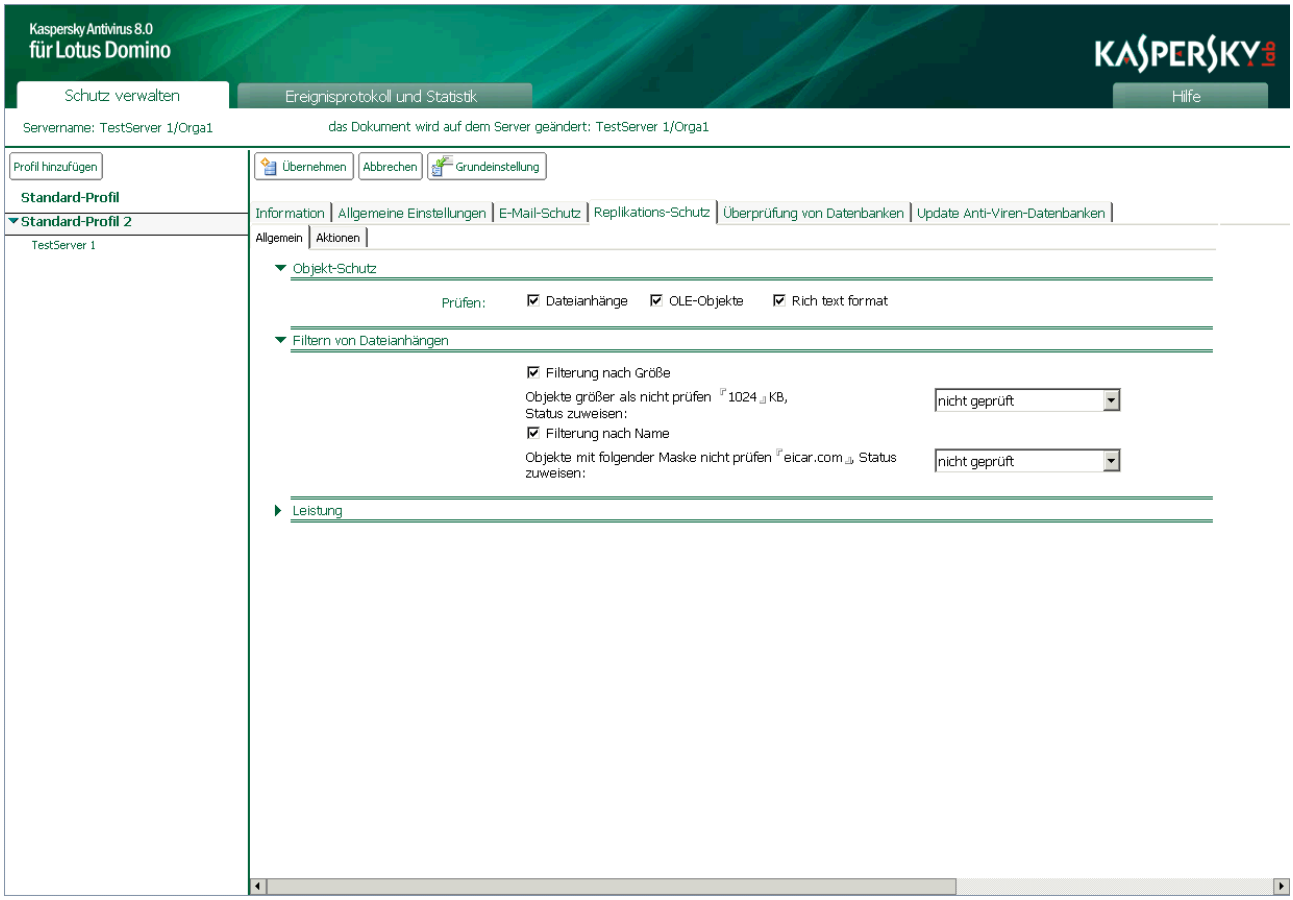


Abbildung 25: Auswahl der Objekte des Replikationsschutzes

4. Damit die Anhangsfilterung durchgeführt wird, setzen Sie folgende Häkchen im Bereich **Filtern von Dateianhängen** (s. Abbildung oben) :

   - **Filterung nach Größe**. Setzen Sie dieses Häkchen, damit Kaspersky Anti-Virus die Dokumentanhangsgröße untersucht. Im **Objekte größer als nicht untersuchen** Feld geben Sie die Objektgröße in Kilobyte (KB) an. Bei einer Überschreitung wird das Objekt ausgefiltert und aus der Anti-Viren-Untersuchung ausgeschlossen. Aus der geöffneten Liste wählen Sie den Status, dementsprechend das Objekt von Kaspersky Anti-Virus verarbeitet werden soll.

   - **Filterung nach Name**. Setzen Sie dieses Häkchen, damit Kaspersky Anti-Virus die Dokumentanhangsnamen untersucht. Im **Objekte mit folgender Maske nicht prüfen** Feld geben Sie die Dateiennamensmasken an, anhand welcher ausgefiltert und von der Anti-Viren-Untersuchung ausgeschlossen wird. Aus der geöffneten Liste wählen Sie den Status, dementsprechend das Objekt von Kaspersky Anti-Virus verarbeitet werden soll.

   > Beim Filtern nach Namen wird nach Groß- und Kleinschreibung unterschieden.

   Sie können mehrere durch**;**" Zeichen voneinander getrennten Masken angeben. Bei der Maskenerstellung verwenden Sie folgende Zeichen: * und ? (s. Abschnitt "Filtern von E-Mail-Anhängen" auf der S. 67).

   Falls das Häkchen nicht gesetzt ist, wird die Filterung entsprechender Objekte nicht durchgeführt.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

UNTERSUCHUNG DER DATENBANKEN

Die Untersuchung der Datenbanken wird planmäßig oder auf manuellen Befehl hin gestartet. Die Untersuchungseinstellungen werden durch ein Profil vorgegeben. Die Anpassung einzelner Einstellungen für einen Server ist nicht vorgesehen. Die Aktivierung und Deaktivierung der Untersuchung der Datenbanken (s. Abschnitt "Untersuchung der Datenbanken aktivieren und deaktivieren" auf der S. 79) ist nur separat für jeden einzelnen Server möglich.

Nach der Programminstallation werden Standardeinstellungen verwendet (s. Abschnitt "Standardmäßiger Serverschutz" auf der S. 49). Sie können sie entsprechend den an den geschützten Domino-Server gestellten Sicherheitsforderungen anpassen. Ein Teil dieser aufgezählten Einstellungen ist standardmäßig deaktiviert oder kann von einem Administrator deaktiviert werden.

Wenn die Anti-Viren-Untersuchung der Datenbanken aktiviert ist, untersucht Kaspersky Anti-Virus standardmäßig die Datenbanken, welche sich im data Ordnerstamm (Ordner der Domino-Server Installation) und allen seinen Unterordnern gesprichert sind. Sie können die Untersuchung der Datenbanken, welche in den Unterordnern des data Ordners bis zum untersten Hierarchieniveau gespeichert sind, aktivieren und deaktivieren.

Kaspersky Anti-Virus ermöglicht es Ihnen, einzelne Datenbanken aus der Untersuchung auszuschließen. Standardmäßig ist die Quarantäne Datenbank aus der Untersuchung ausgeschlossen (kavquarantine.nsf).

Außerdem können Sie die Namensmasken der untersuchten Datenbankdateien angeben (s. Abschnitt "Auswahl von Objekten der Datenbankenüberprüfung" auf der S. 80). In diesem Fall wird Kaspersky Anti-Virus nur die Datenbankendateien untersuchen, welche den Masken entsprechen.

Standardmäßig werden Dokumentfelder im Rich Text Format, Anhänge und eingebettete OLE-Objekte in den Datenbanken auf Vorhandensein von Bedrohungen untersucht.

Sie können die Überprüfung der Anhänge, OLE-Objekte und Inhalt der Rich Text-Felder deaktivieren (s. Abschnitt "Auswahl von Objekten der Datenbankenüberprüfung" auf der S. 80). Sie können auch die Untersuchungsdauer einzelner Objekte beschränken, was die gesamte Leistungsfähigkeit der E-Mailuntersuchung wesentlich steigert (s. Abschnitt "Leistung" auf der S. 89).

Die bei der Untersuchung entdeckten infizierten, möglicherweise infizierten und wegen einer Störung oder Beschädigung nicht untersuchten Objekte werden gemäß den Einstellungen der Datenbanküberprüfung verarbeitet (s. Abschnitt "Aktionen für Objekte im Modus der Datenbankenüberprüfung" auf der S. 82).

Den Anhänge, deren Größe den angegebenen Wert überschreiteten und / oder deren Namen der angegebenen Dateinamensmaske entsprechen, kann eine besondere Verarbeitungsreihenfolge zugewiesen werden (s. Abschnitt " Filtern von Dateianhängen im Modus der Datenbankenüberprüfung" auf der S. 84).

Standardmäßig wird vor der Verarbeitung eine Kopie des Objekts in die Quarantäne verschoben (s. Abschnitt "Quarantäne" auf der S. 91).

Es werden Benachrichtigung über die Überprüfung eines Dokumentes, welches durch Kaspersky Anti-Virus untersucht wurde und die Beschreibung der ausgeführten Aktionen, an die Administratoren gesendet (s. Abschnitt "Benachrichtigungen" auf der S. 109). Informationen über die Untersuchungsergebnisse und ausgeführten Aktionen werden in die Ereignisprotokoll- und Statistikdatenbank eingetragen.

IN DIESEM ABSCHNITT

Untersuchung der Datenbanken aktivieren und deaktivieren 79

Auswahl von Objekten der Datenbankenüberprüfung 80

Aktionen für Objekte im Modus der Datenbankenüberprüfung 82

Filtern von Dateianhängen im Modus der Datenbankenüberprüfung 84

Planmäßige Untersuchung 86

Manuelle Untersuchung 87

UNTERSUCHUNG DER DATENBANKEN AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig ist die Untersuchung der Datenbanken aktiviert und wird beim Hochfahren des Domino-Servers automatisch gestartet. Informationen über den Start der Module, welche die Untersuchung der Datenbanken sichern, werden im Kaspersky Anti-Virus Ereignisprotokoll festgehalten.

Wenn nötig, können Sie die Untersuchung der Datenbanken aktivieren oder deaktivieren. Entsprechende Operationen werden für jeden einzelnen Server separat durchgeführt.

Um die Datenbanküberprüfung zu aktivieren / deaktivieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie im Profilbestand den Server, für den Sie die Untersuchung der Datenbanken aktivieren / deaktivieren möchten.

3. Im Action panel betätigen Sie die **Ändern** Schaltfläche und im Verwaltungsbereich wählen Sie den **Information** Tab (s. Abbildung unten).

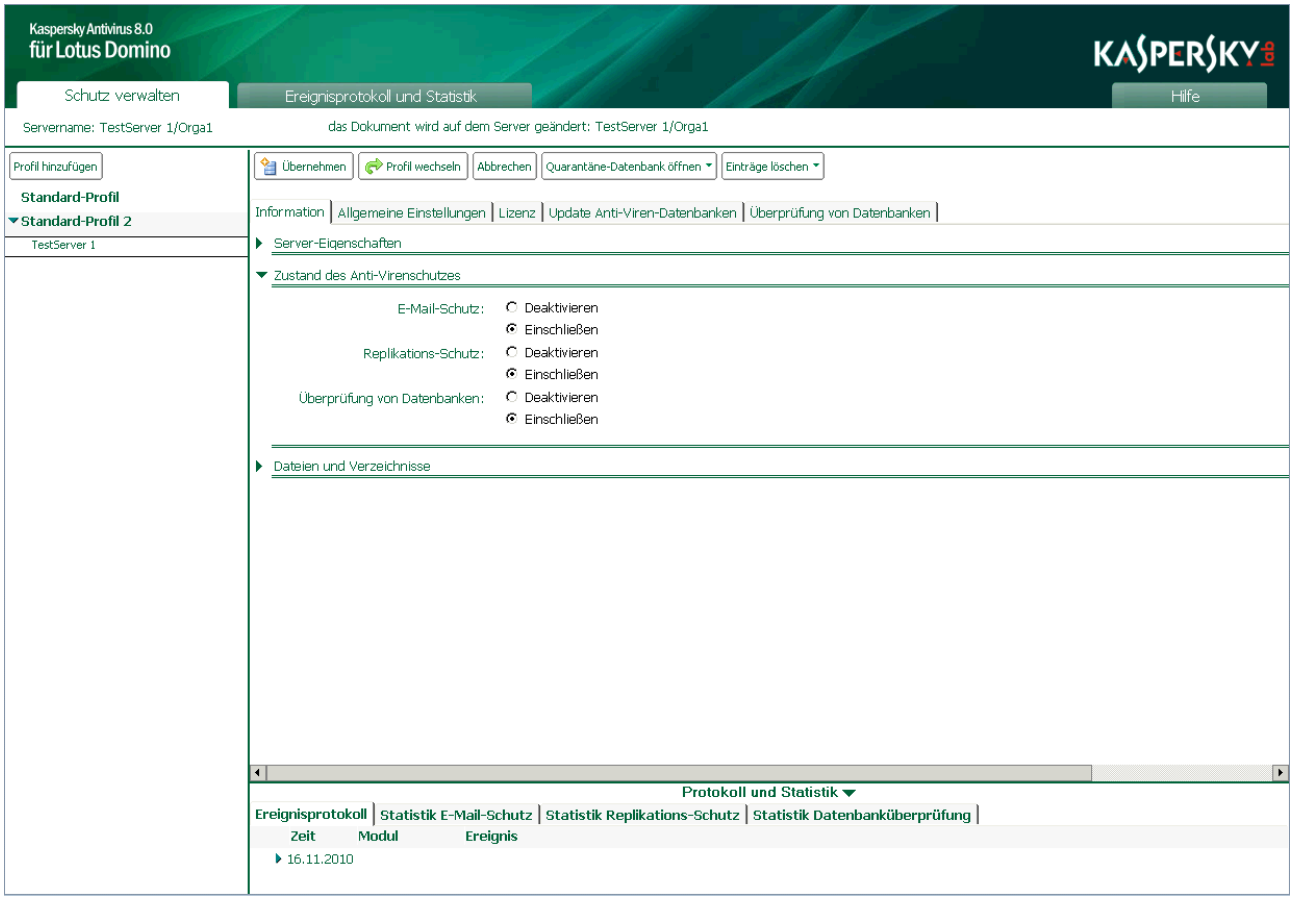


Abbildung 26: Datenbankenüberprüfung aktivieren / deaktivieren

4. Wählen Sie im Bereich **Zustand des Virenschutzes** in der Zeile **Überprüfung von Datenbanken** (s. Abbildung oben) die jeweilige Variante: **Einschließen** oder **Deaktivieren**.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

AUSWAHL VON OBJEKTEN DER DATENBANKENÜBERPRÜFUNG

Standardmäßig untersucht Kaspersky Anti-Virus bei der Anti-Viren-Untersuchung der Datenbanken, die Datenbanken, welche im data Ordner (weiterhin auch in Unterordnern) gespeichert sind. Entsprechend den Untersuchungseinstellungen erstellt Kaspersky Anti-Virus eine Liste der zu untersuchenden Dokumente; anschließend werden die Feldinhalte, alle Anhänge, darunter auch Archive, und eingebettete OLE-Objekte in diesen RTF-Dokumenten untersucht. Wenn nötig, können Sie Untersuchung der aufgezählten Objekte deaktivieren.

Bei der Untersuchung mehrteiliger Archive wird jeder einzelne Archivteil von Kaspersky Anti-Virus als einzelnes Objekt untersucht. Bösartiger Code kann nur dann entdeckt werden, wenn er vollständig in einem der Teile enthalten ist. Falls der Code beispielsweise auf zwei Archivteile verteiltt ist, kann er bei der Untersuchung nicht entdeckt werden. Deshalb wird empfohlen, mehrteilige Archive nach dem Speichern auf der Festplatte mit dem Datei Anti-Virus zu untersuchen.

➧ *Um Objekte für die Anti-Viren-Untersuchung auszuwählen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Betätigen Sie die **Ändern** Schaltfläche im Action panel , und wählen im Verwaltungsbereich im **Überprüfung der Datenbanken** Tab, den Tab **Allgemein** (s. Abbildung unten).

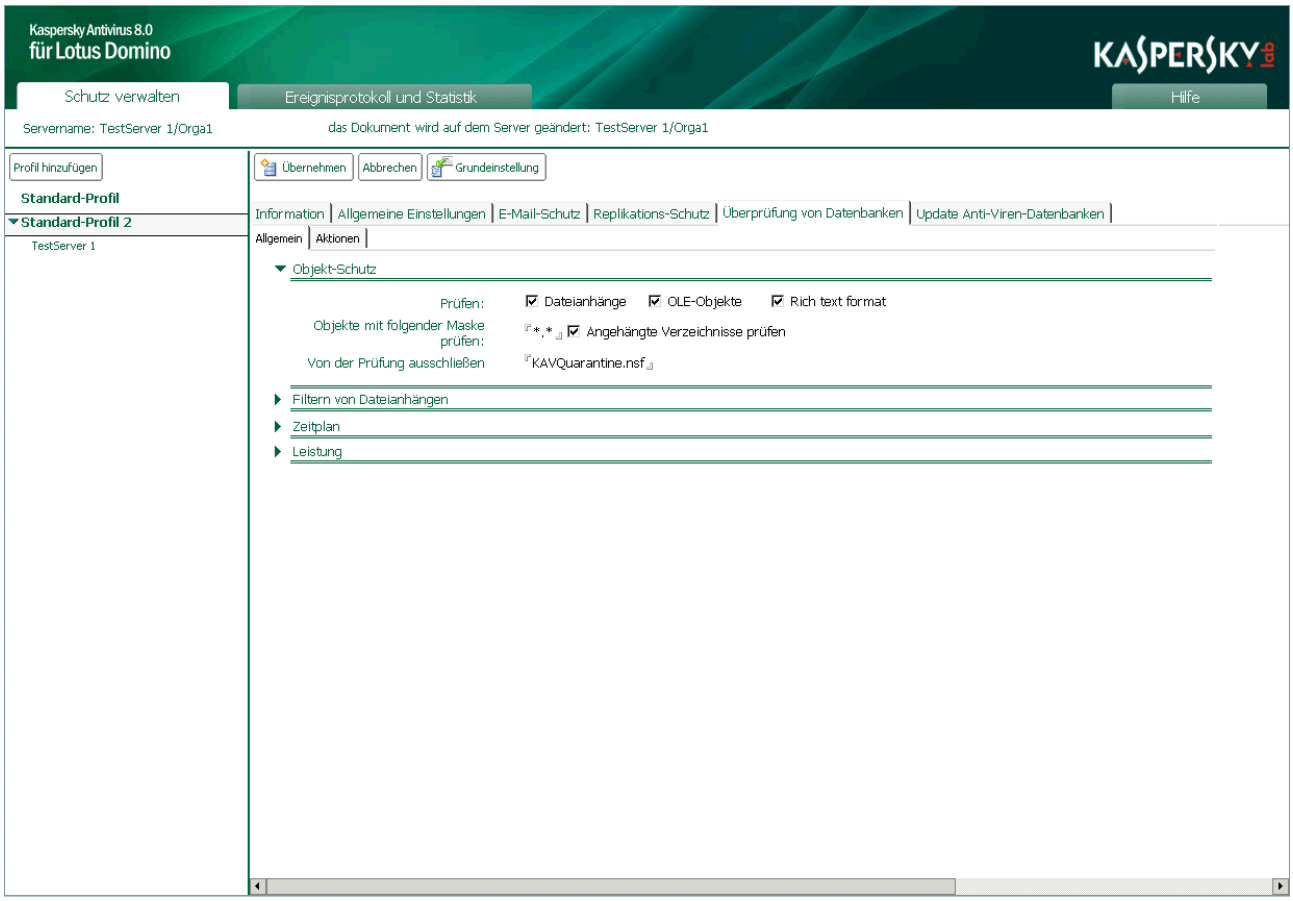


Abbildung 27: Auswahl von Objekten der Datenbankenüberprüfung

4. Damit die Objektuntersuchung ausgeführt wird, setzen Sie folgende Häkchen im Bereich **Objekt-Schutz**:

   - **Dateianhänge** – alle Dokumentanhänge untersuchen.
   - **OLE-Objekte** – alle in der Meldung eingebetteten OLE-Objekte untersuchen.
   - **Rich text format** – Felder des Dokuments im Rich Text Format, untersuchen.

   Wenn das Häkchen nicht gesetzt ist, wird die Untersuchung der entsprechenden Objekte nicht ausgeführt.

5. Im Feld **Objekte mit folgender Maske prüfen** geben Sie die Dateiennamensmasken der Datenbanken an, die von Kaspersky Anti-Virus untersucht werden sollen. Beim der Maskenerstellung können Sie * und ? Zeicheneinsetzen.

6. Setzen Sie das Häkchen bei **Angehängte Verzeichnisse prüfen**, damit Kaspersky Anti-Virus die Datenbanken untersucht, welche in den Unterordnern des data Ordners bis zum untersten Hierarchieniveau gespeichert sind.

   Wenn Sie möchten, dass Kaspersky Anti-Virus nur Datenbanken untersucht, die im data Ordnerstamm gespeichert sind, entfernen Sie dieses Häkchen.

7. Im Fels **Von der Prüfung ausschließen** geben Sie die Namen der Datenbanken an, welche aus der Untersuchung ausgeschlossen werden sollen. Sie können mehrere Angaben tätigen. Verwenden Sie dazu ";" als Trennsymbol. Standardmäßig wird die Quarantäne Datenbank aus der Untersuchung ausgeschlossen (kavquarantine.nsf).

8. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

AKTIONEN FÜR OBJEKTE IM MODUS DER DATENBANKENÜBERPRÜFUNG

Kaspersky Anti-Virus verarbeitet Objekte entsprechend dem Status, der den Objekten nach den Ergebnissen der Anti-Viren-Untersuchung und Filterung der Anhänge zugewiesen wurde (s. Abschnitt "Verarbeitung der Objekte und auf sie angewandte Aktionen" auf der S. 25). Nicht infizierte Objekte werden ohne irgendwelche Änderungen übersprungen. Aktionen an desinfizierbaren, nicht desinfizierbaren, möglicherweise infizierten und nicht untersuchten Objekten können vom Administrator konfiguriert werden.

Die Aktionen, welche das Programm ausführen wird, werden separat mit jedem einzelnen Status bestimmt.

- Es werden folgende standardmäßige Aktionen an den Objekten ausgeführt. Falls das Objekt als desinfizierbar registriert wurde, wird es von Kaspersky Anti-Virus behandelt und das Objekt wird wieder im Dokumentgespeichert.

  Unabhängig von den gewählten-Programmeinstellungen erfolgt die Desinfektion von OLE-Objekten immer durch Löschen.

- Falls das Objekt als nicht desinfizierbar registriert wurde, wird es von Kaspersky Anti-Virus aus dem Dokument gelöscht.

- Falls das Objekt als möglicherweise infiziertes registriert wurde, wird es von Kaspersky Anti-Virus aus dem Dokument gelöscht.

- Falls es nicht gelungen ist, das Objekt zu untersuchen (beispielsweise, weil die Untersuchungsdauer überschritten wurde), wird es von Kaspersky Anti-Virus aus der Meldung gelöscht.

Standardmäßig kann vor der Verarbeitung eine Objektkopie in der Quarantäne Datenbank gespeichert werden (s. S. 91). Informationen über entdeckte Objekte und ausgeführte Aktionen können an die Administratoren gesendet werden (s. Abschnitt "Benachrichtigungen" auf der S. 109) und in der Ereignisprotokoll- und Statistikdatenbank gespeichert werden (s. Abschnitt "Ereignisprotokoll und Statistik" auf der S. 98).

Aktionen, die das Programm ausführen wird, werden in den Untersuchungseinstellungen der Datenbanken separat für jeden einzelnen Status bestimmt.

➧ *Um Aktionen für Objekte zu konfigurieren, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im **Überprüfung der Datenbanken** Tab wählen Sie den Tab **Aktionen** (s. Abbildung unten).

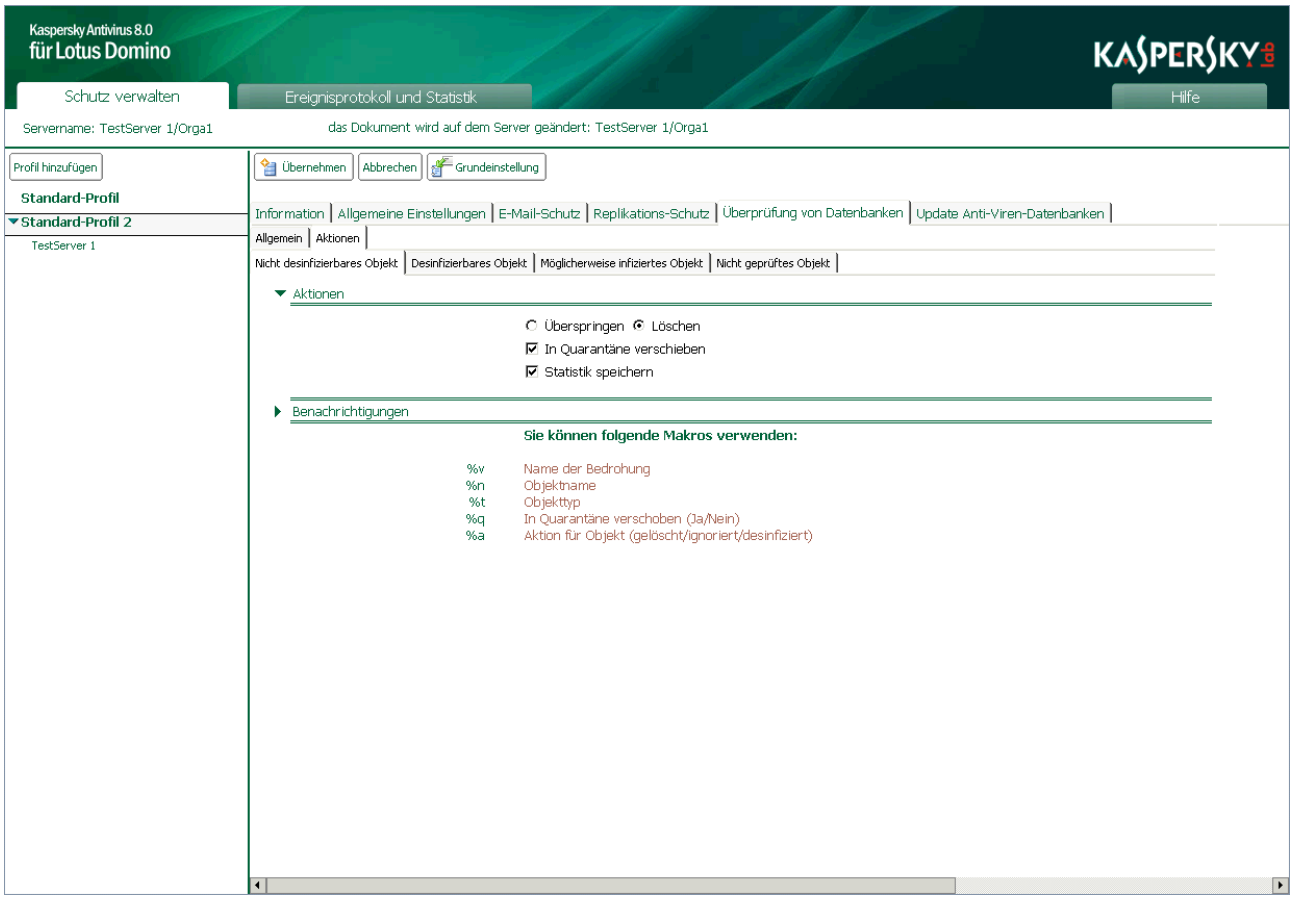


Abbildung 28: Einstellung der Aktionen an nicht desinfizierbaren Objekten im Modus der Datenbankenüberprüfung

4. Im **Aktionen** Tab wählen Sie den Tab, der dem Status des Objekts entspricht, dessen Verarbeitungseinstellungen Sie anpassen möchten. Sie können aus folgenden Tabs wählen

   - **Nicht desinfizierbares Objekt** – Anpassung der Verarbeitungseinstellungen von unheilbaren Objekten.
   - **Desinfizierbares Objekt** – Anpassung der Verarbeitungseinstellungen von desinfizierbaren Objekten.
   - **Möglicherweise infiziertes Objekt** – Anpassung der Verarbeitungseinstellungen von möglicherweise infizierten Objekten.
   - **Nicht geprüftes Objekt** – Anpassung der Verarbeitungseinstellungen von nicht untersuchten Objekten.

5. Im **Aktionen** Bereich (s. Abbildung oben) wählen Sie die Aktion, die an einem entdeckten Objekt ausgeführt werden soll. Setzen Sie zu folgende Häkchen:

   - **In Quarantäne verschieben** – vor der Verarbeitung wird eine Objektkopie in der Quarantäne Datenbank gespeichert.

     In Quarantäne wird nur das Objekt selbst verschoben. Ein Dokument, welches das Objekt beherbergt, wird nicht in Quarantäne verschoben.

   - **Statistik speichern** – Information über entdeckte Objekte und ausgeführte Aktionen werden an den Orten,welche im Feld **Information speichern**, im Tab **Allgemeine Einstellungen** angegeben sind, gespeichert. Falls mehrere Orte gleichzeitig zur Informationsaufbewahrung ausgewählt werden, wird die Information an den angegebenen Orten der Informationsaufbewahrung auch gleichzeitig eingetragen.

- **In die Konsole** (Systemprotokoll Domino log.nsf);
- **Ins Protokoll**;
- **In Datei** (Dateiname auf Grundeinstellung server.log).

6. Im **Benachrichtigungen** Bereich (s. Abbildung unten) passen Sie die Einstellungen an, aufgrund welcher die Benachrichtigungen über entdeckte Objekte und ausgeführte Aktionen geschrieben werden (s. Abschnitt "Benachrichtigungen" auf der S. 109).

7. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

FILTERN VON DATEIANHÄNGEN IM MODUS DER DATENBANKENÜBERPRÜFUNG

Bei der Untersuchung der Datenbanken schließt Kaspersky Anti-Virus die Anhänge, welche die Filtereinstellungen treffen, aus der Anti-Viren-Untersuchung aus. Bei der Untersuchung der Datenbanken wird dasselbe Prinzip der Anhangsfilterung wie das bei der im E-Mail-Schutz Modus verwendet. Standardmäßig wird im Modus der Überprüfung der Datenbanken keine Filterung von Anhängen durchgeführt.

Standardmäßig wird den ausgefilterten Objekten der Status *nicht untersucht* zugewiesen und an ihnen werden die in den Einstellungen der Datenbanken-Untersuchung für diese Kategorie vorgegebenen Aktionen ausgeführt.

Um die Anhangsfilterung zu konfigurieren, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, [jnm ult- Einstellungen Sie ändern möchten.

3. Betätigen Sie die **Ändern** Schaltfläche im Action panel , und wählen im Verwaltungsbereich im **Überprüfung der Datenbanken** Tab, den Tab **Allgemein** (s. Abbildung unten).

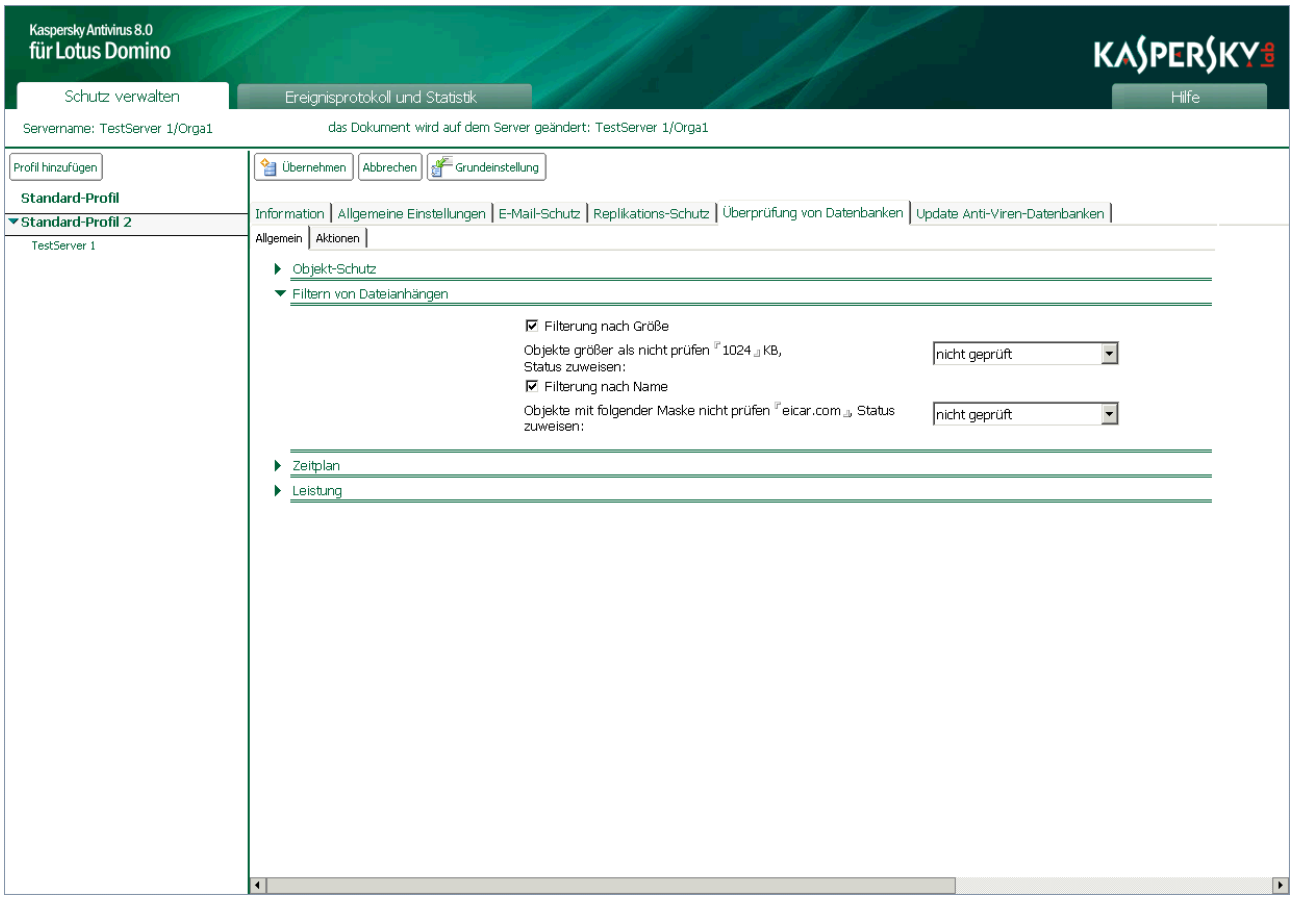


Abbildung 29: Anpassung der Anhangsfilterung im Modus der Datenbankenüberprüfung

4. Damit die Anhangsfilterung durchgeführt wird, setzen Sie folgende Häkchen im Bereich **Filtern von Dateianhängen** (s. Abbildung oben) :

   - **Filterung nach Größe**. Setzen Sie dieses Häkchen, damit Kaspersky Anti-Virus die Dokumentanhangsgröße untersucht. Im **Objekte größer als nicht untersuchen** Feld geben Sie die Objektgröße in Kilobyte (KB) an. Bei einer Überschreitung wird das Objekt ausgefiltert und aus der Anti-Viren-Untersuchung ausgeschlossen. Aus der geöffneten Liste wählen Sie den Status, dementsprechend das Objekt von Kaspersky Anti-Virus verarbeitet werden soll.

   - **Filterung nach Name**. Setzen Sie dieses Häkchen, damit Kaspersky Anti-Virus die Dokumentanhangsnamen untersucht. Im **Objekte mit folgender Maske nicht prüfen** Feld geben Sie die Dateiennamensmasken an, anhand welcher ausgefiltert und von der Anti-Viren-Untersuchung ausgeschlossen wird. Aus der geöffneten Liste wählen Sie den Status, dementsprechend das Objekt von Kaspersky Anti-Virus verarbeitet werden soll.

   Beim Filtern nach Namen wird nach Groß- und Kleinschreibung unterschieden.

   Sie können mehrere durch";" Zeichen voneinander getrennten Masken angeben. Bei der Maskenerstellung verwenden Sie folgende Zeichen: * und ?(s. Abschnitt "Filtern von E-Mail-Anhängen" auf der S. 67).

   Falls das Häkchen nicht gesetzt ist, wird die Filterung entsprechender Objekte nicht durchgeführt.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

PLANMÄßIGE UNTERSUCHUNG

Kaspersky Anti-Virus führt die Untersuchung der Datenbanken nach dem Untersuchungszeitplan aus. Sie können die Einstellungen des Untersuchungszeitplans nur für eine Server-Gruppe durch ein Profil einstellen.

Um die Einstellungen des Untersuchungszeitplans anzupassen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Betätigen Sie die Schaltfläche **Ändern** im Action panel und wählen im Verwaltungsbereich wählen den Tab **Überprüfung von Datenbanken** Tab (s. Abbildung unten).

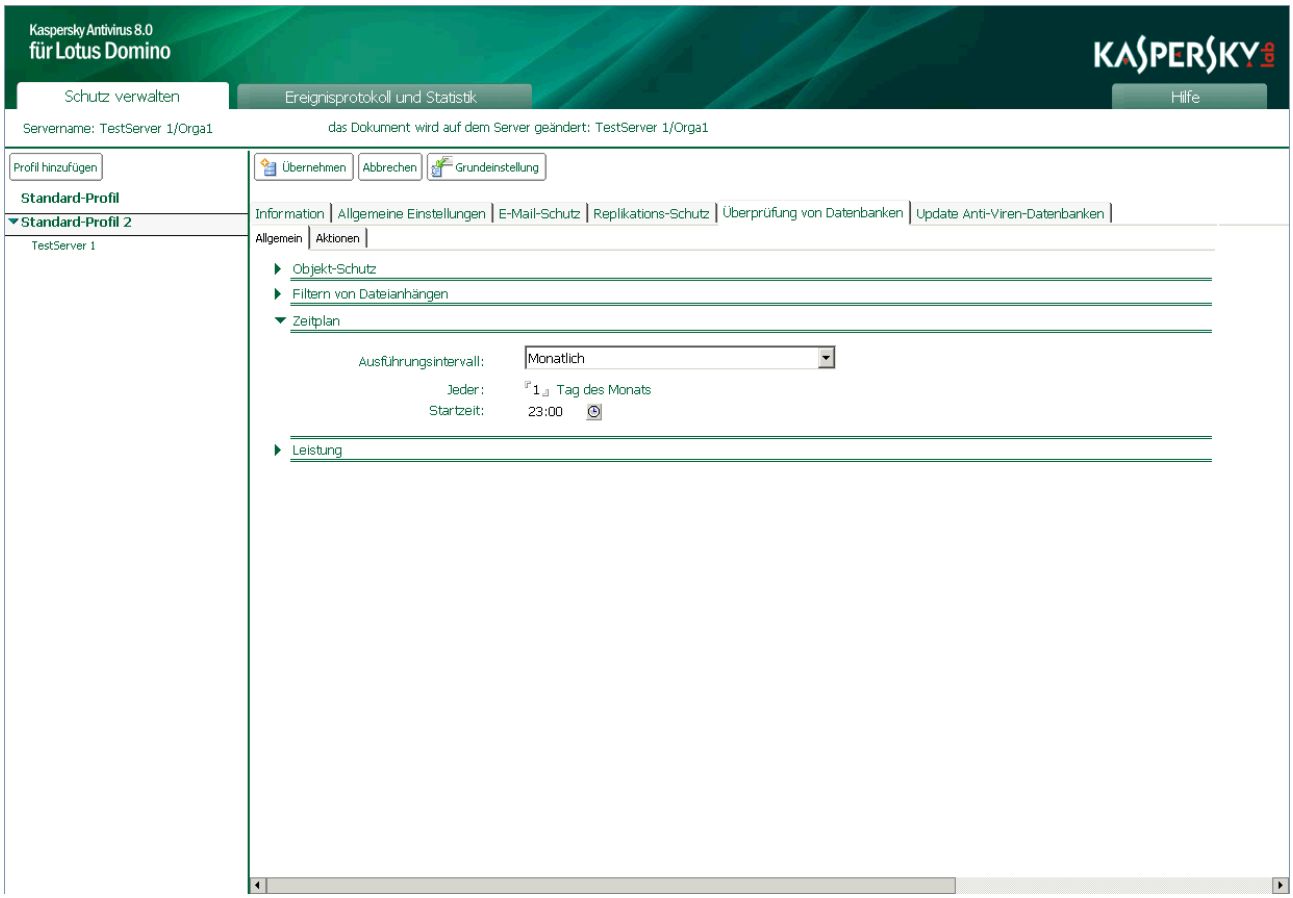


Abbildung 30: Einstellung des Zeitplans der Datenbankenüberprüfung

4. Im Bereich **Zeitplan** (s. Abbildung oben) wählen Sie in der geöffneten Liste **Ausführungsintervall** eine der folgenden Angaben:

   - **Wöchentlich** – die Untersuchung der Datenbanken wird wöchentlich an den angegebenen Tagen zur angegebenen **Startzeit** ausgeführt. Setzen Sie Häkchen an den Wochentagen, an welchen die Untersuchung der Datenbanken gestartet wird und geben Sie im Feld **Startzeit** die nötigen Angaben an. Format **Std.:Min**.

   - **Monatlich** – die Untersuchung der Datenbanken werden einmal pro Monat am angegeben Tag zur angegebenen **Startzeit** ausgeführt. Geben Sie die nötige Angabe im Feld **Startzeit** ein. Format **Std.:Min**.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

MANUELLE UNTERSUCHUNG

Sie können die manuelle Untersuchung der Datenbanken nur für einen Server aktivieren. Für eine Server-Gruppe ist dieser Untersuchungsmodus nicht vorgesehen.

Die manuelle Untersuchung kann in dem Fall aktiviert werden, wenn die planmäßige Untersuchung deaktiviert ist.

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie im Profilbestand den Server, dessen Überprüfung Sie möchten.

3. Im Verwaltungsbereich wählen Sie den Tab **Überprüfung der Datenbanken** (s. Abbildung unten). Im Tab werden Informationen über Datum und Zeit des letzten und nächsten Starts der Datenbankenüberprüfung nach den Zeitplanvorgaben dargestellt.

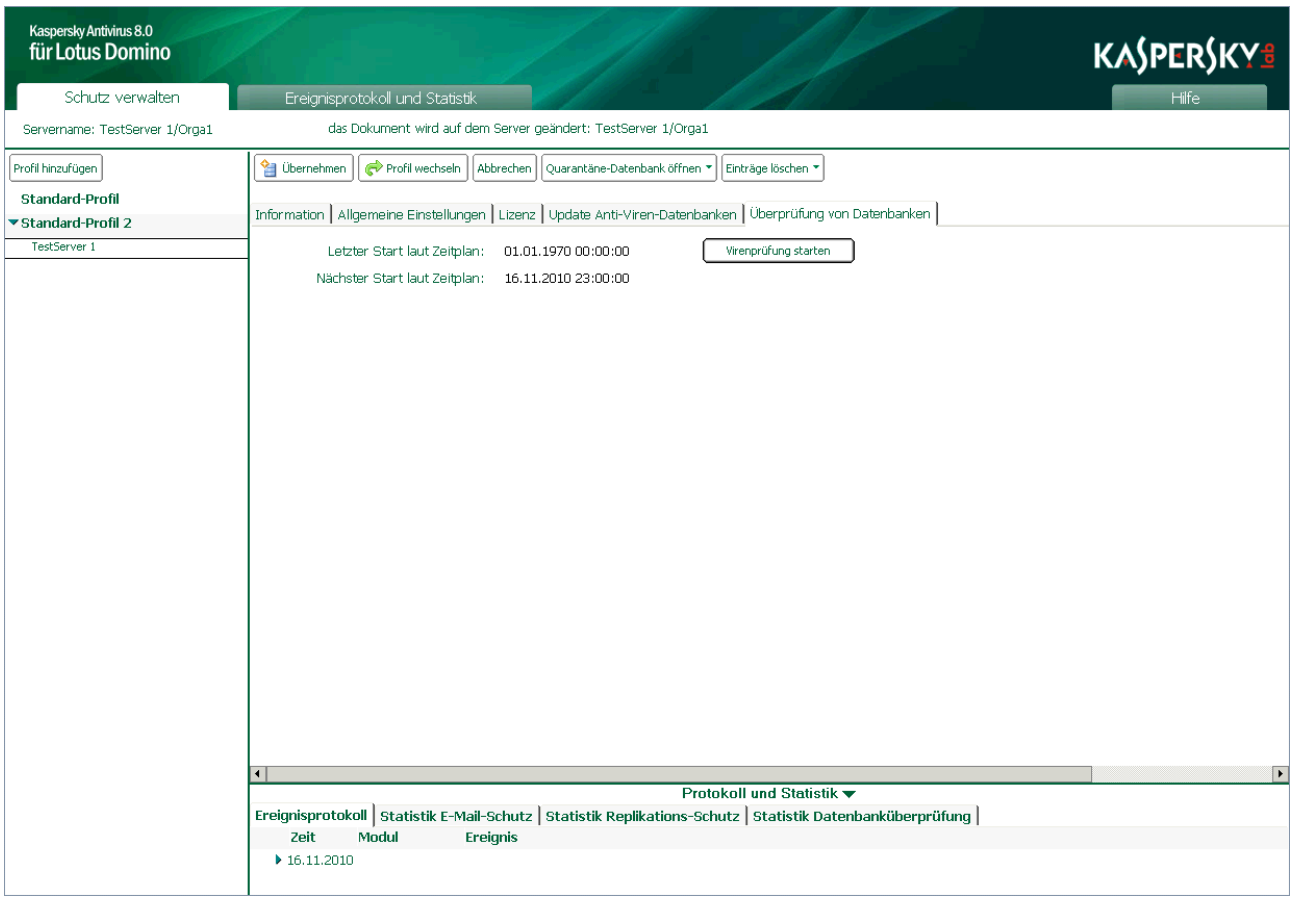


Abbildung 31: Datenbankenüberprüfung manuell starten

4. Betätigen Sie die Schaltfläche **Virenprüfung starten**, um die Untersuchung der Datenbanken zu starten.

Das Update kann auch aus der Befehlszeile gestartet werden (s. Abschnitt "Arbeit im Server-Konsolen-Modus" auf der S. 122).

LEISTUNG

Kaspersky Anti-Virus bietet Ihnen eine Option, mit welcher Sie die Programmleistung bei der Objektuntersuchung mittels folgender Einstellungen regeln können:

- *Untersuchungsdauer einzelner Objekte.* Falls die Objektuntersuchung länger als der vorgegebene Wert dauert, wird sie angehalten. Dem Objekt wird der Status *nicht untersucht* zugewiesen, und das Programm geht zur Untersuchung des nächsten Objekts über.

- *Objektuntersuchung im Arbeitsspeicher.* Falls die Objektgröße den vorgegebenen Wert nicht überschreitet, wird das Objekt im Arbeitsspeicher des Servers untersucht, ohne auf der Festplatte gespeichert zu werden.

Sie können die Programmleistungseinstellungen anpassen. Für jede Schutzkomponente werden die Einstellungen der Untersuchungsleistung separat konfiguriert.

➧ *Um die Einstellungen des Untersuchungszeitplans anzupassen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich im Tab **E-Mail-Schutz / Replikations-Schutz / Überprüfung von Datenbanken** wählen Sie den Tab **Allgemein** (s. Abbildung unten).

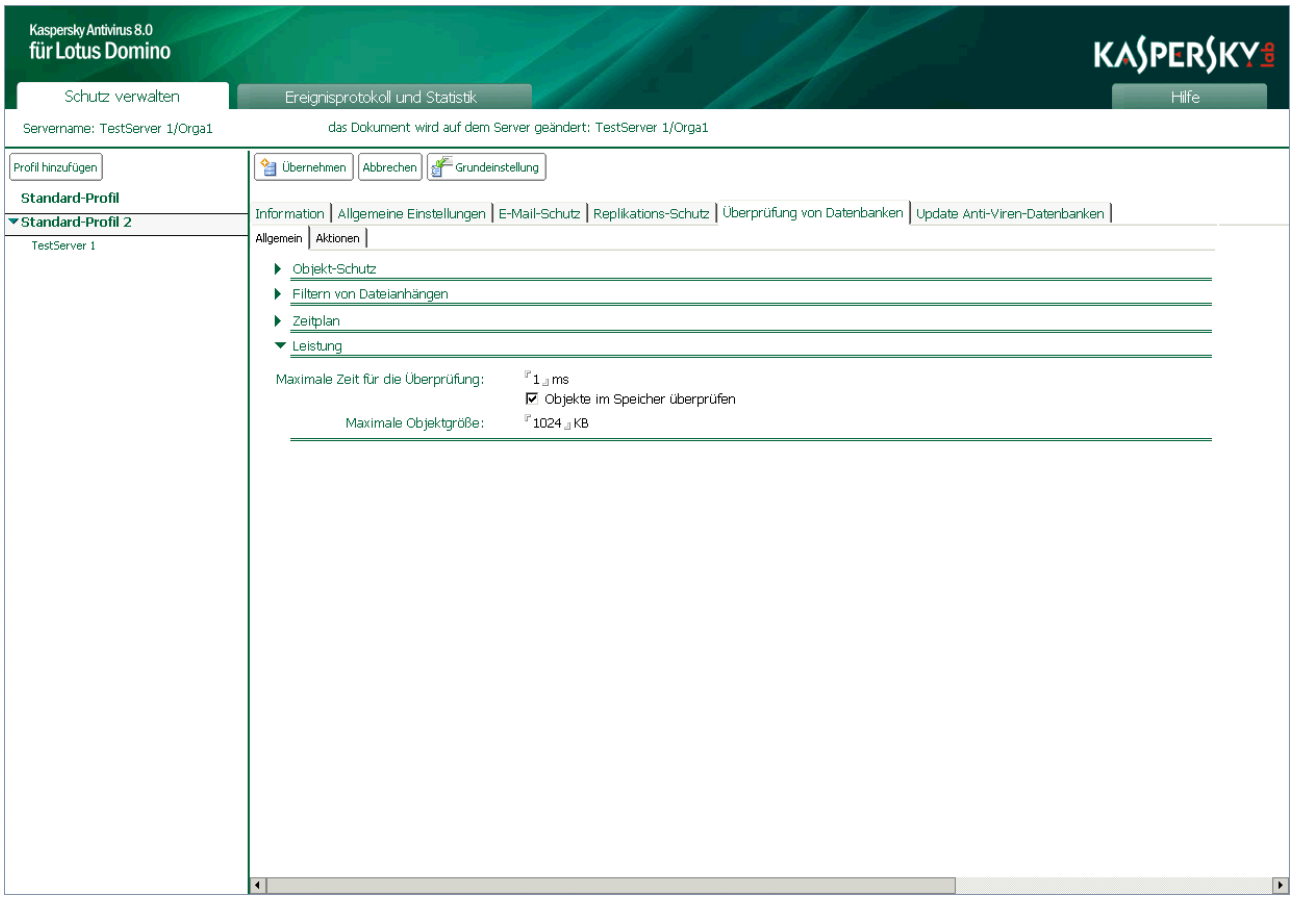


Abbildung 32: Anpassung der Leistungseinstellungen der Datenbankenüberprüfung

4. Im Bereich **Leistung** passen Sie die Einstellungen an, demnach die Untersuchung ausgeführt wird. Dazu gehen Sie wie folgt vor:

   - Im Feld **Maximale Zeit für die Überprüfung** geben Sie die maximale Untersuchungsdauer eines Objekts in Millisekunden vor. Standardmäßig beträgt die maximale Untersuchungsdauer 300 Millisekunden.

   - Setzen Sie das Häkchen bei **Objekte im Speicher überprüfen** und geben im Feld **Maximale Objektgröße** die maximale Größe eines untersuchten Objekts in Kilobyte (KB) an. Standardmäßig beträgt die maximale Objektgröße 1024 KB.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

QUARANTÄNE

Entsprechend den Einstellungen des E-Mail-, Replikationsschutzes und den Untersuchungseinstellungen der Datenbanken, werden Kopien der bei Anti-Viren-Untersuchungen entdeckten Objekte, in die Quarantäne Datenbank gespeichert – kavquarantine.nsf.

Die Quarantänedatenbank wird zur Aufbewahrung der in die Quarantäne verschobenen Objekte verwendet. Die Quarantänedatenbank wird auf jedem der geschützten Server als Kopie aufbewahrt und enthält die Originalobjekte, die durch den Anti-Viren-Task des Servers in die Quarantäne verschoben wurden. Bei der Programminstallation können Sie wählen, ob die Quarantäne-Objekte in allen Repliken aufbewahrt werden nur Objekte des eigenen Servers enthalten.

Standardmäßig werden Objekte in die Quarantäne verschoben, die nach der Anti-Viren-Untersuchung als nicht desinfizierbar, desinfizierbar, möglicherweise infiziert und nicht untersucht registriert wurden. Welche Kategorien von Objekten in die Quarantäne verschoben werden, wird in den Einstellungen für den E-Mail-Schutz, den Replikationsschutz und die Untersuchung der Datenbanken für jede Objektkategorie einzeln festgelegt.

Eine Option mittels welcher die Objekte manuell in Quarantäneverschoben werden, ist nicht vorgesehen.

Die kavquarantine.nsf Datenbank wird bei der Programminstallation im Ordner von Kaspersky Anti-Virus erstellt (standardmäßiger Ordner kavdatabases). Zugriff auf die in die Quarantäne verschobenen Objekte ist nur durch die Benutzeroberfläche der Verwaltungscenter Datenbank möglich (s. Abschnitt "Programmoberfläche" auf der S. 38).

Zur besseren Übersichtlichkeit und Informationssuche werden die in die Quarantäne verschobenen Objekte in verschiedenen Teilen dargestellt (s. Abschnitt "Einsicht der in die Quarantäne verschobenen Objekte" auf der S. 92).

Standardmäßig beträgt die maximale Frist der Objektaufbewahrung in der Quarantäne 30 Tage. Sie können die Aufbewahrungsfrist der in die Quarantäne verschobenen Objekte in den Servereinstellungen anpassen (s. Abschnitt "Quarantäne-Einstellungsanpassung" auf der S. 96). Falls eine Beschränkung der Objektaufbewahrungsfrist eingestellt ist (s. Abschnitt "Quarantäne-Einstellungsanpassung" auf der S. 96), werden die entsprechenden Objekte nach Ablauf der vorgegebenen Zeitdaueraus der Datenbank gelöscht. Wenn nötig, können Sie Objekte manuell aus der Quarantäne Datenbank löschen.

Der Gesamtumfang der in der Quarantäne aufbewahrten Objekte wird durch die physikalischen Größe der Datenbank beschränkt. Die maximale Größe der Quarantäne Datenbank beträgt 64 GB. Beim Erreichen dieses Wertes werden keine weiteren Objekte mehr in Quarantäne verschoben. In diesem Fall empfehlen wir Ihnen die Objekte, welche zuvor in die Quarantäne verschoben wurden, manuell zu entfernen (s. Abschnitt "Aktionen an den in die Quarantäne verschobenen Objekte" auf der S. 94), oder, um die Quarantäne zu leeren, die Objektaufbewahrungseinstellungen zu ändern.

IN DIESEM ABSCHNITT

Einsicht der in die Quarantäne verschobenen Objekte 92

Aktionen an den in die Quarantäne verschobenen Objekte 94

Quarantäne-Einstellungsanpassung 96

EINSICHT DER IN DIE QUARANTÄNE VERSCHOBENEN OBJEKTE

Die Einsicht von Objekten in der Quarantäne erfolgt durch die Benutzeroberfläche der Verwaltungscenterdatenbank. Die Objekte, die als Folge der Untersuchung der E-Mails, der Replikationen und der Datenbanken in die Quarantäne verschoben wurden, werden in verschiedenen Teilen dargestellt.

Sie können folgende Typen der Objekte, die in die Quarantäne verschoben wurden, einsehen: E-Mails, Datenbanken und Replikationen. Jeder dieser Objekttypen wird in einem einzelnen Fenster angezeigt. Sie können die Quarantäne-Einträge sofort für alle Server gleichzeitig öffnen.

Um die in die Quarantäne verschobenen Objekte und Informationein zu sehen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie einen beliebigen Server aus dem Bestand eines beliebigen Profils.

   Falls es bei der Installation in den Bereitstellungseinstellungen kein Häkchen bei **Objekte der Quarantäne in allen Replikationen speichern** gesetzt wurde, so werden in jedem Replikat nur die Einträge eines (laufenden) Servers aufbewahrt.

3. Betätigen Sie die Schaltfläche **Quarantäne-Datenbank öffnen** im Action panel und wählen eine der folgenden Angaben aus der Liste:

   - **E-Mails**.
   - **Datenbanken**.
   - **Replikationen**.

Demzufolge werden im Verwaltungsbereich Quarantäne-Einträge für alle Server dargestellt (s. Abbildung unten). Einträge über die in die Quarantäne verschobenen E-Mails werden nach dem Eintragungsdatum und den E-Mail-Adressen der Absender gruppiert. Einträge über Objekte, die infolge der Untersuchung von Replikationen und Datenbanken in die Quarantäne verschoben wurden, werden nach den Eintragungsdatum und Namen der Datenbanken, in welchen die untersuchten Dokumente gespeichert sind, gruppiert.

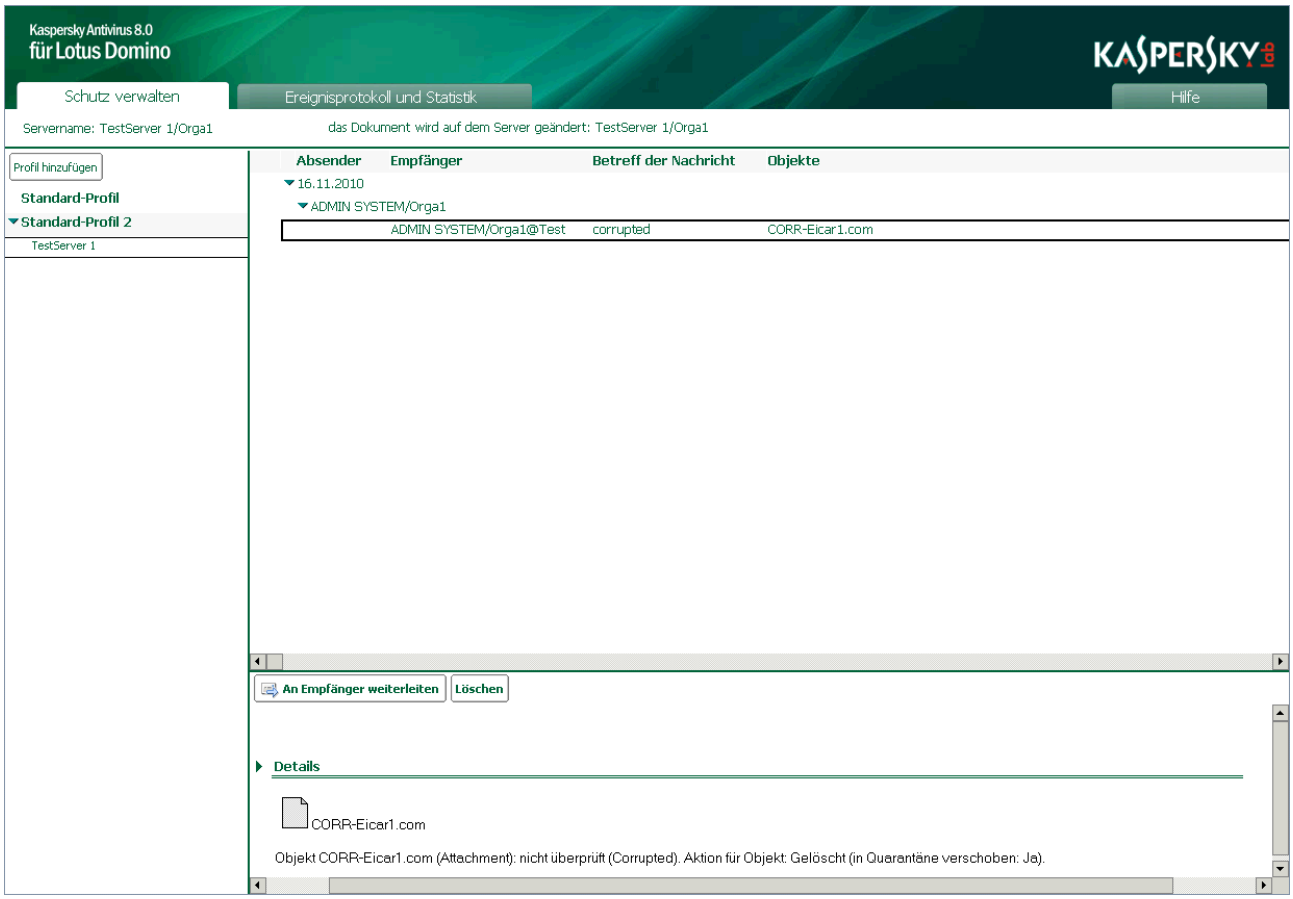


Abbildung 33: Einsehen der in die Quarantäne verschobenen Objekte

Um die komplette Liste der gruppierten Einträge zu öffnen, betätigen Sie ▶. Um die Liste zusammenzuklappen, betätigen ▼.

Sie können auch zusätzliche Informationen von jedem der in die Quarantäne verschobenen Objekte einsehen.

Dazu wählen Sie das Objekt mit einem Klick aus der Liste von Einträgen, wenn Sie Informationen darüber einsehen möchten. Demzufolge werden im Ansichtsbereich im Bereich **Details** folgende Informationen über das ausgewählte Objekt dargestellt:

- Für E-Mails:
  - **Datum** – Datum und Zeit der Objekteintragung in Quarantäne.
  - **Servername** – Name des Servers, auf dem die Untersuchung ausgeführt wurde.
  - **Absender** – E-Mail-Adresse des Meldungsabsenders.
  - **Empfänger** – E-Mail-Adressen der Meldungsempfänger.
  - **Kopie** – E-Mail-Adressen der Empfänger der Meldungskopie.
  - **Blind Copy –** E-Mail-Adressen der Empfänger der Blindkopie.

- **Betreff der Nachricht** – Betreff der E-Mail, in welcher eine Bedrohung entdeckt wurde.
- Anhangsliste.
- Textinformationen, welche den Objektnamen, den Namen der entdeckten Bedrohung und eine Liste der am Objekt ausgeführten Aktionen enthält.

- Für replizierte Dokumente und Dokumente der Datenbanken:
  - **Datum** – Datum und Zeit der Objekteintragung in Quarantäne.
  - **Server** – Name des Servers, auf welchem die Untersuchung ausgeführt wurde.
  - **Modul** – Name des Moduls, welches die Untersuchung ausgeführt hat und das Objekt in die Quarantäne verschoben hat.
  - **Datenbank** – Name der Datenbank, in der sich das Objekt befindet.
  - **Modifiziert** – Name des Benutzers, der die letzte Änderungen ins Dokument eingetragen hat, und Name des Servers, auf dem sie ausgeführt wurde; Eintragsformat: **Benutzername / Servername**.
  - **Dokument** – Nummer (Name) des Dokuments auf dem Domino-Server, in dem eine Bedrohung entdeckt wurde.
  - Anhangsliste.
  - Textinformationen, welche den Objektnamen, den Namen der entdeckten Bedrohung und eine Liste der am Objekt ausgeführten Aktionen enthält.

AKTIONEN AN DEN IN DIE QUARANTÄNE VERSCHOBENEN OBJEKTE

Sie können an den in die Quarantäne verschobenen Objekte folgende Aktionen durchführen:

- Objekte manuell löschen;
- Einträge, die älter als die angegebene Frist, in Tagen sind, löschen;
- E-Mails an Empfänger übersenden.

Nach dem Ablauf der Aufbewahrungsfrist, die in den Servereinstellungen vorgegeben ist, werden Objekte von Kaspersky Anti-Virus aus der Quarantäne Datenbank automatisch gelöscht.

Um Objekte aus der Quarantäne Datenbank zu löschen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie einen beliebigen Server aus dem Bestand eines beliebigen Profils.
3. Betätigen Sie die Schaltfläche **Quarantäne-Datenbank öffnen** im Action panel und wählen eine der folgenden Angaben aus der Liste:
   - **E-Mails**.
   - **Datenbanken**.
   - **Replikationen**.

Demzufolge werden im Verwaltungsbereich Quarantäne-Einträge für alle Server dargestellt.

4. Um die Liste der gruppierten Einträge zu öffnen, betätigen Sie das Zeichen .

5. Wählen Sie das Objekt mit einem Klick aus der Liste, welches Sie aus der Quarantäne Datenbank löschen wollen. Danach betätigen Sie im Ansichtsbereich die Schaltfläche **Löschen** (s. Abbildung unten).

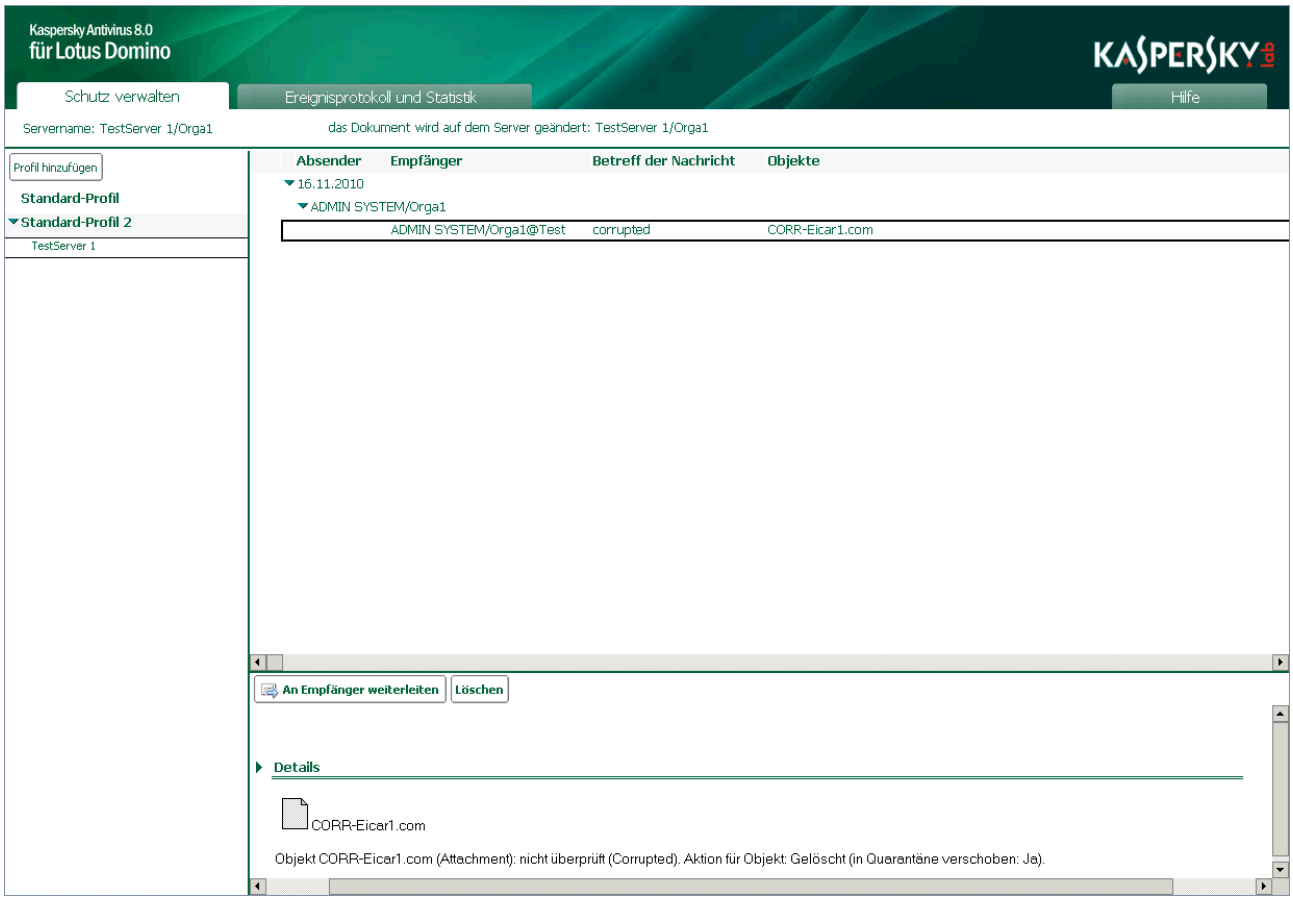


Abbildung 34: Objekte aus der Quarantäne löschen

Mit den **Ctrl** und **Shift** Tasten können Sie mehrere Objekte wählen.

Um eine E-Mail aus der den Empfänger zu übersenden, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie einen beliebigen Server aus dem Bestand eines beliebigen Profils.

3. Betätigen Sie die Schaltfläche **Quarantäne-Datenbank öffnen** im Action panel und wählen **E-Mail-Nachrichten** aus der geöffneten Liste.

   Demzufolge werden die Einträge über die in die Quarantäne verschobenen E-Mails für alle Server im Verwaltungsbereich dargestellt.

4. Um die Liste der gruppierten Einträge zu öffnen, betätigen Sie das Zeichen .

5. Wählen Sie mit einem Klick die E-Mail aus der Liste, die Sie an den Empfänger übersenden wollen. Danach betätigen Sie die Schaltfläche **An Empfänger weiterleiten** im Ansichtsbereich.

   Mit den **Ctrl** und **Shift** Tasten können Sie mehrere Objekte wählen.

Um Objekte aus Quarantäne zu löschen, welche das Zeitlimit zur Aufbewahrung überschritten haben, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie einen beliebigen Server aus dem Bestand eines beliebigen Profils.

3. Betätigen Sie die Schaltfläche **Einträge löschen** im Action panel und wählen **Quarantäne** aus der geöffneten Liste.

4. Im geöffneten Fenster geben Sie die Anzahl der Tage an, nach welchen die Einträge gelöscht werden sollen. Betätigen Sie die Schaltfläche **OK**.

   Demzufolge werden die Einträge, deren Aufbewahrungsfrist die angegebene Dauer überschreiten, aus der Quarantäne Datenbank gelöscht.

QUARANTÄNE-EINSTELLUNGSANPASSUNG

Sie können die Aufbewahrungsfrist der in die Quarantäne verschobenen Objekte in den Servereinstellungen anpassen.

Um die Aufbewahrungsfrist der in die Quarantäne verschobenen Objekte anzupassen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie den Server aus dem Profilbestand, dessen einstellungen Sie anpassen möchten.

3. Betätigen Sie die **Ändern** Schaltfläche im Action panel , und wählen im Verwaltungsbereich im Überprüfung der Datenbanken Tab, den Tab **Allgemeine Einstellungen** (s. Abbildung unten).

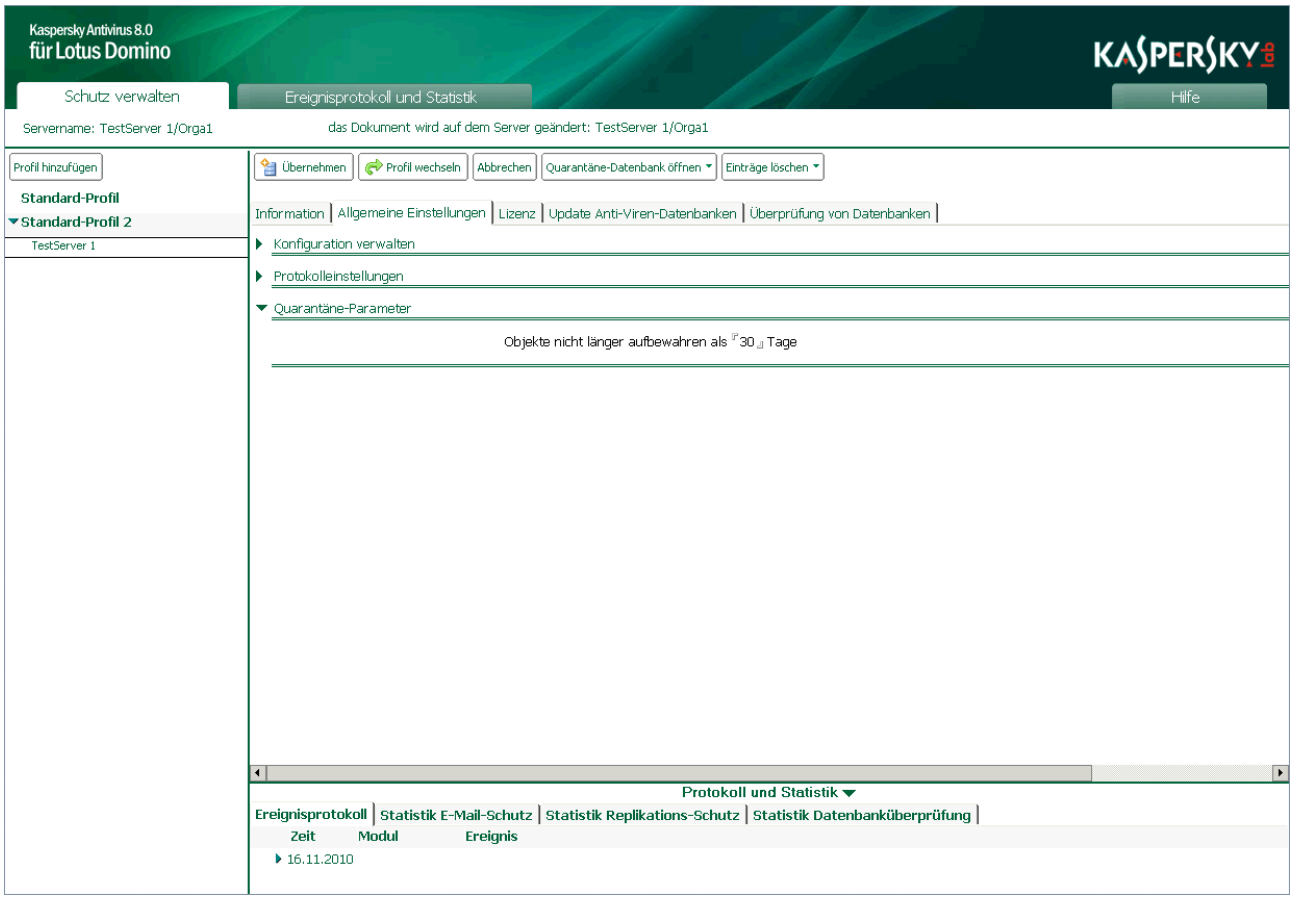


Abbildung 35: Anpassung der Quarantäne-Einstellungen

4. Im Bereich **Quarantäne Einstellungen** geben Sie die Aufbewahrungsfrist der in die Quarantäne verschobenen Objekte in Tagen an. Standardmäßig beträgt die Objektaufbewahrungsfrist 30 Tage.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

In den Einstellungen des E-Mail-, Replikations- und Datenbankschutzes können Sie bestimmen, welche Kategorien der Objekte in die Quarantäne verschoben werden sollen. Die Einstellungsanpassung wird für jede Objektkategorie separat ausgeführt.

Wenn Sie möchten, dass nach den Ergebnissen der Anti-Viren-Untersuchung nicht nur die Objekte der E-Mails, sondern die ganze E-Mail in die Quarantäne verschoben werden soll, setzen Sie das Häkchen in den Schutzparametern im **Erweitert** Tab bei **Ganze Nachricht in Quarantäne verschieben** (s. Abschnitt "**Aktionen an den E-Mail-Objekten**" auf der S. 62).

EREIGNISPROTOKOLL UND STATISTIK

Kaspersky Anti-Virus ermöglicht es Ihnen, die Informationen über die im Programmdurchlauf festgestellten Ereignisse sowie statistische Information über die infolge der Anti-Viren-Untersuchung entdeckten Bedrohungen und ausgeführten Aktionen zu speichern.

Die Ereignisprotokoll- und Statistikdatenbank wird zur Aufbewahrung der Ereignisse, welche während des Betriebs von Kaspersky Anti-Virus registriert wurden, sowie statistischen Informationen über die Ergebnisse der Objektüberprüfungen und ausgeführten Aktionen, verwendet. Die Ereignisprotokoll- und Statistikdatenbank wird als Replikat verbreitet und auf jedem der geschützten Server der Infrastruktur aufbewahrt. Sie enthält kumulative Statistiken über alle Ereignisse auf allen geschützten Servern. Alle Änderungen werden durch den Standardmechanismus der Replikation nach dem Zeitplan und der Topologie verbreitet.

Standardmäßig werden die Informationen in der Ereignisprotokoll- und Statistikdatenbank – kaveventslog.nsf - aufbewahrt.

Die Ereignisprotokoll- und Statistikdatenbank wird zur Aufbewahrung der Ereignisse, welche während des Betriebs von Kaspersky Anti-Virus registriert wurden, sowie statistischen Informationen über die Ergebnisse der Objektüberprüfungen und ausgeführten Aktionen, verwendet. Die Ereignisprotokoll- und Statistikdatenbank wird als Replikat verbreitet und auf jedem der geschützten Server der Infrastruktur aufbewahrt. Sie enthält kumulative Statistiken über alle Ereignisse auf allen geschützten Servern. Alle Änderungen werden durch den Standardmechanismus der Replikation, dem Zeitplan und der Topologie entsprechend verbreitet.

Im Fall des eines verteilten Schemas von Kaspersky Anti-Virus werden die Information über alle geschützten Server in der kaveventslog.nsf aufbewahrt.

Die kaveventslog.nsf Datenbank wird bei der Programminstallation im Ordner der Kaspersky Anti-Virus Installation erstellt (standardmäßiger Ordner: kavdatabases). Zugriff zu Informationen, welche in der Ereignisprotokoll- und Statistikdatenbank gespeichert sind, ist nur durch die Elemente der Benutzer-Oberfläche der Verwaltungscenter Datenbank möglich. Das Einsehen und Löschen der Information ist durch Kaspersky Anti-Virus möglich (s. Abschnitt "Die Ereignisprotokoll- und Statistikdatenbank einsehen" auf der S. 105).

Im Ereignisprotokoll werden Informationen, welche die Aktivität von Kaspersky Anti-Virus und seinen Modulen auf dem Niveau der Domino-Serveraufgaben darstellt, gespeichert (s. Abschnitt "Programm-Architektur" auf der S. 21).

Die Vollständigkeit der im Ereignisprotokoll festgestellten Informationen wird durch die **Detailgenauigkeit** bestimmt. Standardmäßig werden nur die wichtigsten Informationen über die Arbeit aller Kaspersky Anti-Virus Module gespeichert: Ereignisse von kritischer Wichtigkeit, die auf Probleme im Programmdurchlauf oder Sicherheitslücken im Serverschutz hinweisen.

Das Level der Detailgenauigkeit der Informationen im Protokoll, der Ort für die Darstellung der Information über Ereignisse und die Aufbewahrungsfrist der Einträge in der kaveventslog.nsf Datenbank werden durch die Ereignisprotokolleinstellungen bestimmt (s. Abschnitt "Einstellungen des Ereignisprotokolls" auf der S. 99). Durch ein Profil können Sie die Ereignisprotokolleinstellungen für eine Server-Gruppe oder auch für jeden Server einzeln anpassen. Eine Datei zur Speicherung des Ereignisprotokolls kann nur in den Servereinstellungen angegeben werden. Die Änderung dieser Einstellung durch ein Profil ist nicht vorgesehen.

In die Statistik werden Informationen über die Ergebnisse der Anti-Viren-Objektuntersuchung, entdeckte Bedrohungen und an den Objekten ausgeführte Aktionen geschrieben. Für jede Schutzkomponente wird eine einzelne Statistik geführt. Welche Informationen in der Statistik gespeichert werden, wird durch das Profil in den Einstellungen für den E-Mail-Schutz, den Replikationsschutz und der Untersuchung von Datenbanken festgelegt. Standardmäßig werden von der Untersuchung erhaltene Informationen über desinfizierbare, nicht desinfizierbare und möglicherweise infizierte Objekte sowie Informationen über nicht untersuchte Objekte mit der Angabe von der Ursache gespeichert.

Standardmäßig werden die Einträge in der Ereignisprotokoll- und Statistikdatenbank für 30 Tage aufbewahrt. Nach dem Ablauf der vorgegebenen Zeitdauer werden die Einträge automatisch gelöscht. Sie können die Aufbewahrungsfrist von Ereignissen und der Statistik durch ein Profil oder durch die Servereinstellungen ändern (s. Abschnitt "Einstellungen des Ereignisprotokolls" auf der S. 99, "Statistikeinstellungen" auf der S. 101).

Für jeden geschützten Server ist eine Option vorgesehen, um Informationen über diesen Server manuell aus der Ereignisprotokoll- und Statistikdatenbank zu löschen (s. Abschnitt "Löschen der Information aus der Ereignisprotokoll- und Statistikdatenbank" auf der S. 104).

Ereignisse, die auf dem geschützten Server während des laufenden Betriebs festgestellt wurden, können auch in der Domino-Server-Konsole dargestellt und in eine Logdatei geschrieben werden(s. Abschnitt "Einstellungen des Ereignisprotokolls" auf der S. 99). Standardmäßig werden fünf zyklisch wiederbeschreibbare Logdateien mit dem Namen server.log_N, wobei N die Ordnungsnummer der Log-Datei darstellt, verwendet. Die Log-Dateien befinden sich auf dem geschützten Server im Dienstordner von Kaspersky Anti-Virus logs und enthalten nur für diesen Server Informationen.

Sie können die Anzahl der verwendeten Log-Dateien, ihre Namen und die zulässige Größe mit Hilfe der Parameter in der Konfigurationsdatei notes.ini ändern (s. Abschnitt "Einstellungsverwaltung der Konfigurationsdatei notes.ini" auf der S. 28).

IN DIESEM ABSCHNITT

Einstellungen des Ereignisprotokolls 99

Statistikeinstellungen 101

Löschen der Information aus der Ereignisprotokoll- und Statistikdatenbank 104

Die Ereignisprotokoll- und Statistikdatenbank einsehen 105

EINSTELLUNGEN DES EREIGNISPROTOKOLLS

Kaspersky Anti-Virus bietet Ihnen eine Option, die Protokolleinstellungen für eine Server-Gruppe (durch ein Profil) oder für jeden Server einzeln in den Servereinstellungen anzupassen.

Standardmäßig werden die Ereignisprotokolleinstellungen vom Profil, welches den geschützten Server einschließt, bestimmt. Damit Kaspersky Anti-Virus die in den Servereinstellungen vorgegebenen Werte verwendet, muss im Tab **Allgemeine Einstellungen** das Häkchen bei **Profil-Einstellungen verwenden** entfernt werden.

➧ *Um die Ereignisprotokolleinstellungen anzupassen, gehen Sie wie folgt vor:*

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie ein Profil, falls Sie die Ereignisprotokolleinstellungen für eine Server-Gruppe anpassen möchten, oder den Server, falls Sie die Ereignisprotokolleinstellungen für einen einzelnen Server einstellen.
3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und im Verwaltungsbereich wählen Sie den Tab **Allgemeine Einstellungen** (s. Abbildung unten).

Falls Sie die Ereignisprotokolleinstellungen für einen einzelnen Server anpassen, entfernen Sie das Häkchen bei **Profil- Einstellungen verwenden** im Bereich **Protokolleinstellungen**. Wenn das Häkchen gesetzt ist, werden die Einstellungen des Ereignisprotokolls und der Statistik nicht dargestellt (s. Abbildung unten). Sollen die vom Profil vorgegebenen Einstellungswerte für den Server verwendet werden, muss das Häkchen bei **Profil-Einstellungen verwenden** gesetzt werden.

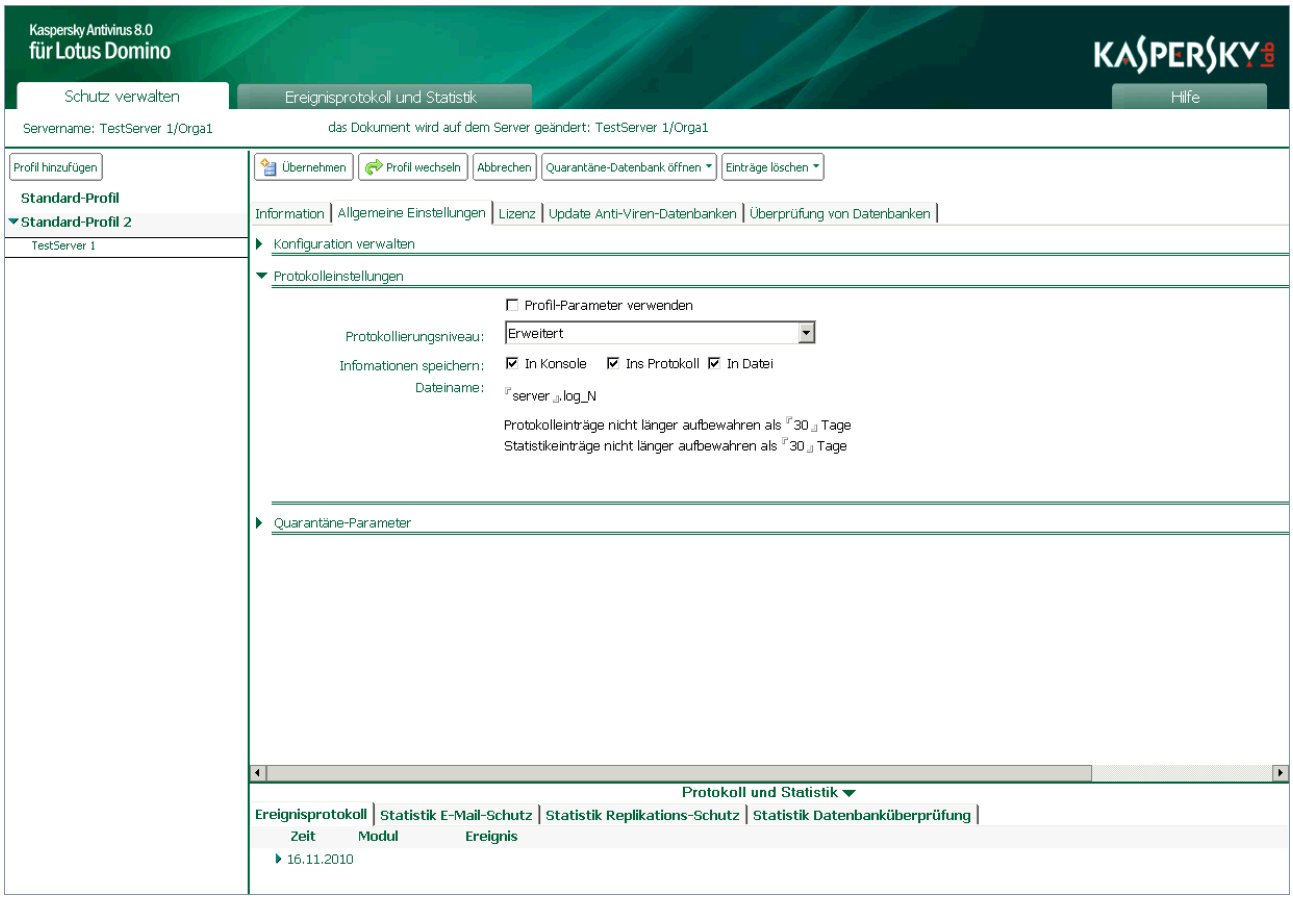


Abbildung 36: Einstellungsanpassung des Ereignisprotokolls für einzelne Server

4. Im **Protokolleinstellungen** Bereich (s. Abbildung oben) geben Sie folgende Einstellungswerte an:

   - Detaillierungsgrad der im Protokoll festgestellten Informationen. Dafür wählen Sie in der geöffneten Liste **Protokollierungsniveau** eine der folgenden Angaben:

     - **Standard** – **Kritische Ereignisse** sowie Ereignisse, die unbedingt beachtet werden müssen, da sie wichtige Situationen im Programmdurchlauf darstellen (beispielsweise, **Fehler beim Verbinden zur Updatequelle**) . Diese Angabe ist standardmäßig gesetzt. i KAVDefaultLogLevel – 0.

     - **Erweitert** – Ereignisse von kritischer Wichtigkeit registrieren, die auf Sicherheitslücken im Serverschutz oder auf Probleme beim Programmdurchlauf verweisen. Es werden Informationen über die Arbeit aller Kaspersky Anti-Virus Module registriert. KAVDefaultLogLevel – 1.

     - **Debug** – **Kritische Ereignisse**, **Wichtige Ereignisse** und Referenz-Typ E-Mails. Z.b: **Objekt ist nicht infiziert**, **Modul-Update heruntergeladen**. KAVDefaultLogLevel – 2.

   - Auswahl des Aufbewahrungsortes der Informationen über festgestellte Ereignisse. Dafür setzen Sie im **Information speichern** Bereich folgende Häkchen:

     - **Ins Protokoll** – Informationen über Ereignisse werden in der Ereignisprotokoll- und Statistikdatenbank (kaveventslog.nsf) gespeichert. Sie können das Ereignisprotokoll durch die Benutzeroberfläche der Verwaltungscenter Datenbank einsehen (s. Abschnitt "Die Ereignisprotokoll- und Statistikdatenbank einsehen" auf der S. 105).

Die kaveventslog.nsf Datenbank wird bei der Programminstallation im Ordner der Kaspersky Anti-Virus Installation erstellt (standardmäßiger Ordner: kavdatabases).

- **In die Konsole** – Informationen über Ereignisse während des Betriebs von Kaspersky Anti-Virus werden an die Domino-Server-Konsole weitergegeben. Auch werden Angaben über die laufende Programmsitzung angeboten. Der Detailgenauigkeit der Informationen wird von der gewählten Detailisierungsgrad bestimmt.

- **In Datei** – Informationen über Ereignisse werden in eine Logdatei eingetragen. Standardmäßig werden fünf zyklisch wiederbeschreibbare Logdateien mit dem Namen server.log_N, wobei N die Ordnungsnummer der Log-Datei darstellt, verwendet. Die Logdateien befinden sich auf dem geschützten Server im Dienstordner von Kaspersky Anti-Virus logs und enthalten nur für diesen Server Informationen.

  Der logs Ordner wird bei der Programminstallation erstellt und befindet sich unter folgender Adresse: Für Betriebssysteme der Microsoft Windows Reihe – im Binärdateienordner des Domino-Servers (standardmäßiger Pfad: C:\Program Files\IBM\Lotus\Domino\kavcommon). Für Betriebssysteme der Linux Reihe – im Datenordner des Domino-Servers (standardmäßiger Pfad: /local/notesdata/kavcommon).

  Die Größe der Log-Dateien wird in der Konfigurationsdatei notes.ini (Parameter KAVLogFileSize) festgelegt. Um eine Datei einzusehen, verwenden Sie die Standardmittel zur Ansicht einer Textdatei des Microsoft Windows oder Linux Betriebssystems.

  In den Servereinstellungen können Sie eine andere Datei zur Aufbewahrung der Informationen über Ereignisse während des Betriebs von Kaspersky Anti-Virus angeben. Dafür geben Sie im Feld **Dateiname** den Namen der Datei an, in welche Sie Informationen über Ereignisse aufbewahren wollen. Danach wird im Kaspersky Anti-Virus logs Dienstordner die angegebene Datei erstellt. Die Änderung des Dateinamens durch ein Profil ist nicht vorgesehen.

- Aufbewahrungsfrist von Ereignisprotokolleinträgen in der kaveventslog.nsf Datenbank. Im Feld **Protokolleinträge nicht länger aufbewahren als** geben Sie die Dauer in Tagen an, nach deren Ablauf die Einträge über Ereignisse aus der Ereignisprotokoll- und Statistikdatenbank automatisch gelöscht werden. Standardmäßig beträgt die Aufbewahrungsfrist von Informationen 30 Tage.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Falls Sie die Update-Einstellungen für eine Server-Gruppe anpassen möchten, können Sie die standardmäßigen Einstellungswerte wiederherstellen. Dazu betätigen Sie die Schaltfläche **Grundeinstellung**.

Die Einstellungen des Ereignisprotokolls können auch in der ini Datei vorgenommen werden (s. Abschnitt "Einstellungsverwaltung der Konfigurationsdatei notes.ini" auf der S. 28).

STATISTIKEINSTELLUNGEN

Kaspersky Anti-Virus ermöglicht es Ihnen, für jede einzelne Schutzkomponente Einzelstatistiken über entdeckte Bedrohungen und ausgeführte Aktionen zu führen. Standardmäßig werden von der Untersuchung erhaltene Informationen über desinfizierbare, nicht desinfizierbare und möglicherweise infizierte Objekte sowie Informationen über nicht untersuchte Objekte mit der Angabe von der Ursache gespeichert.

Welche Informationen in der Statistik gespeichert werden, wird durch das Profil in den Einstellungen den E-Mail-Schutz, den Replikationsschutz und die Untersuchung von Datenbanken festgelegt. Die Anpassung einzelner Einstellungen der Speicherung der Statistiken für einen Server ist nicht vorgesehen.

Die Aufbewahrungsfrist der statistischen Informationen in der Ereignisprotokoll- und Statistikdatenbank kann durch ein Profil für eine Server-Gruppe, aber auch in den Servereinstellungen für jeden einzelnen Server bestimmt werden. Standardmäßig beträgt die Angabe 30 Tage und wird vom Profil, zu welchem der geschützte Server gehört, bestimmt. Damit Kaspersky Anti-Virus die in den Servereinstellungen vorgegebenen Werte verwendet, muss im Tab **Allgemeine Einstellungen** das Häkchen bei **Profil-Einstellungen verwenden** entfernt werden.

Um die Aufbewahrungsfrist der statistischen Informationen anzupassen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, wenn Sie die Statistikeinstellungen für eine Server-Gruppe anpassen möchten oder den Server, wenn Sie die Statistikeinstellungen für einen einzelnen Server anpassen möchten.

3. Betätigen Sie die Schaltfläche **Ändern** im Action panel und wählen den Tab **Allgemeine Einstellungen** aus dem Verwaltungsbereich (s. Abbildung unten).

Falls Sie die Statistikeinstellungen für einen einzelnen Server anpassen möchten, entfernen Sie das Häkchen bei **Profil-Einstellungen verwenden** im Bereich **Protokolleinstellungen**. Wenn das Häkchen gesetzt ist, werden die Einstellungen des Ereignisprotokolls und der Statistik nicht dargestellt (s. Abbildung unten). Sollen die vom Profil vorgegebenen Einstellungswerte für den Server verwendet werden, muss das Häkchen bei **Profil-Einstellungen verwenden** gesetzt werden.

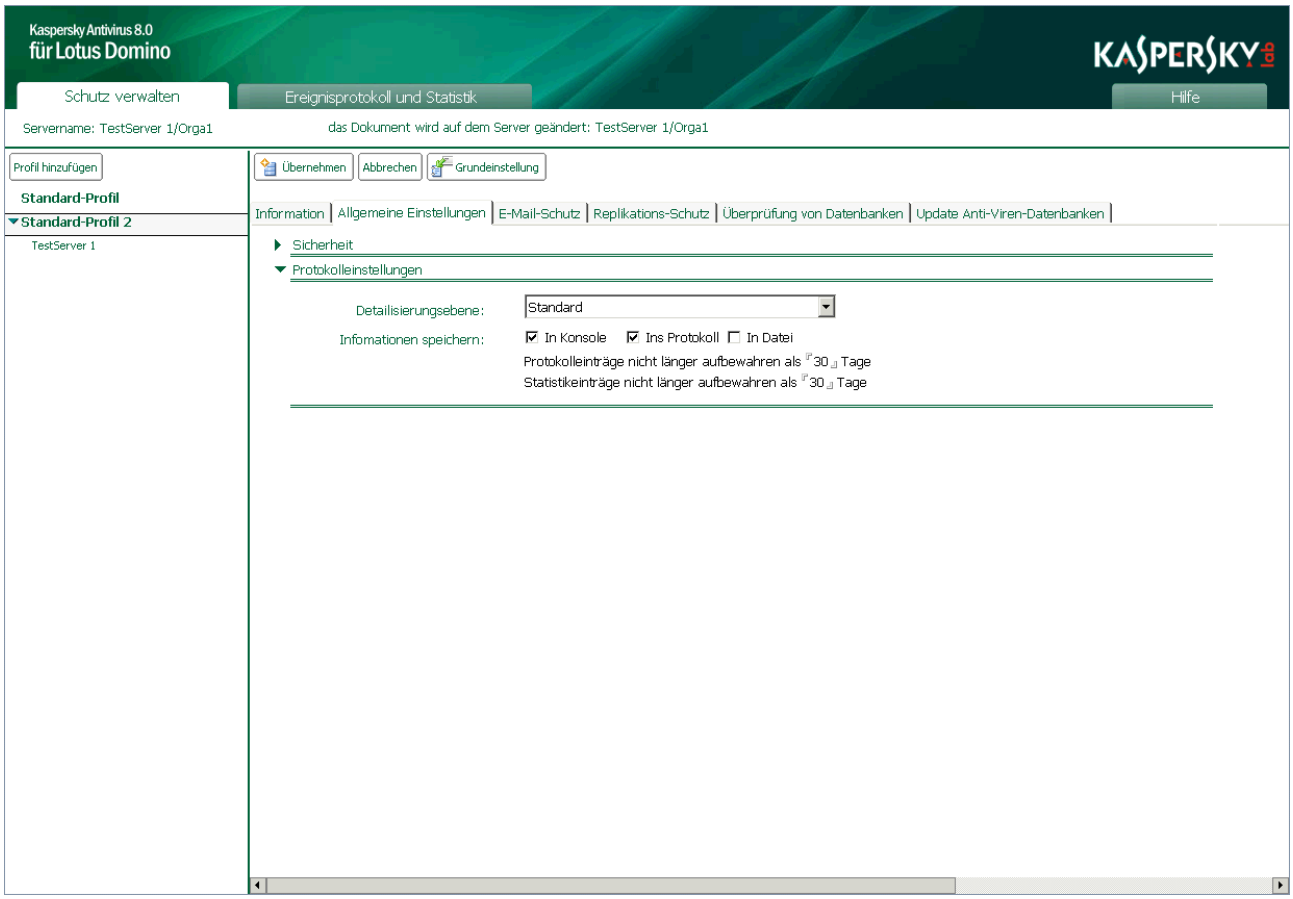


Abbildung 37: Einstellung der Dauer der Statistikaufbewahrung

4. Im **Protokolleinstellungen** Bereich im Feld **Statistikeinträge nicht länger aufbewahren als**, geben Sie die Dauer in Tagen an, nach deren Ablauf Einträge aus der Ereignisprotokoll- und Statistikdatenbank automatisch gelöscht werden (kaveventslog.nsf).

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

Um zu bestimmen, welche statistischen Informationen in die Ereignisprotokoll- und Statistikdatenbank gespeichert werden, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Betätigen Sie die Schaltfläche **Ändern** im Action panel, und wählen im Verwaltungsbereich im Tab **E-Mail-Schutz** / **Replikations-Schutz** / **Überprüfung von Datenbanken**, den Tab **Aktionen** (s. Abbildung unten).

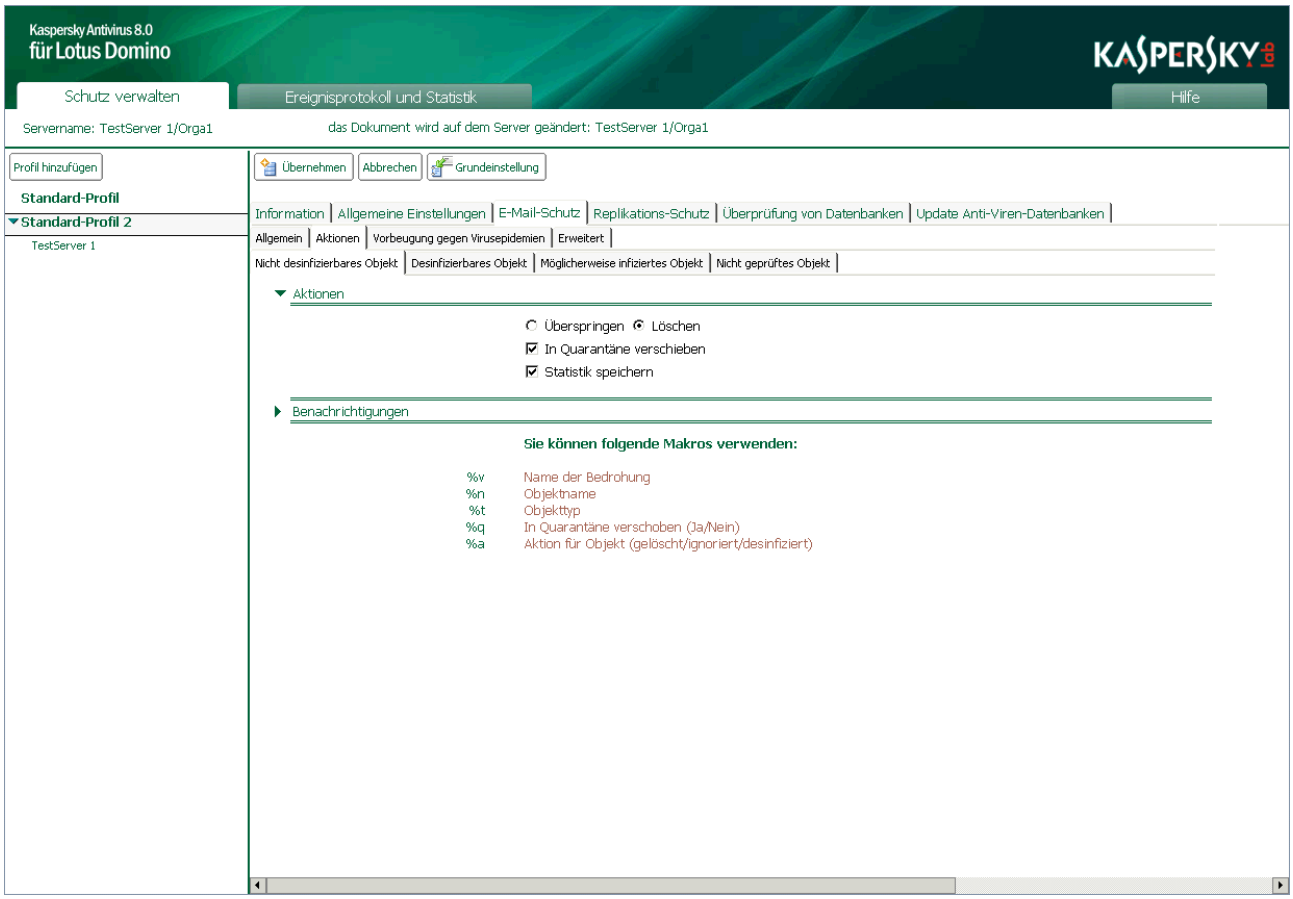


Abbildung 38: Anpassung der Einstellungen der Statistikaufbewahrung

4. Im Tab **Aktionen** wählen Sie den Tab, der dem Status der Objekte, deren Informationen Sie in der Ereignisprotokoll- und Statistikdatenbank aufbewahren wollen, entspricht. Sie können aus folgenden Tabs wählen

   - **Nicht desinfizierbares Objekt**.
   - **Desinfizierbares Objekt**.
   - **Möglicherweise infiziertes Objekt**.
   - **Nicht geprüftes Objekt**.

5. Im gewählten Tab im Bereich **Aktionen** setzen Sie das Häkchen bei **Statistik speichern**, damit die Informationen über entdeckte Objekte und ausgeführte Aktionen in der Ereignisprotokoll- und Statistikdatenbank gespeichert werden. Wenn es nicht nötig ist, die Informationen zu speichern, entfernen Sie das Häkchen.

6. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Falls Sie die Update-Einstellungen für eine Server-Gruppe anpassen möchten, können Sie die standardmäßigen Einstellungswerte wiederherstellen. Dazu betätigen Sie die Schaltfläche **Grundeinstellung**.

LÖSCHEN DER INFORMATION AUS DER EREIGNISPROTOKOLL- UND STATISTIKDATENBANK

Nach Ablauf der Frist, die in den Einstellungen des Ereignisprotokolls und der Statistik angegeben wurden, werden die Ereignisse automatisch aus der Ereignisprotokoll- und Statistikdatenbank gelöscht. Wenn nötig, können Sie die Einträge auch manuell entfernen. Das Löschen wird für jeden einzelnen Server separat ausgeführt.

Um Einträge der Ereignisprotokoll- und Statistikdatenbank manuell zu löschen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie den Server aus dem Profilbestand , für welchen Sie Einträge aus dem Ereignisprotokoll- und der Statistikdatenbank löschen wollen (s. Abbildung unten).

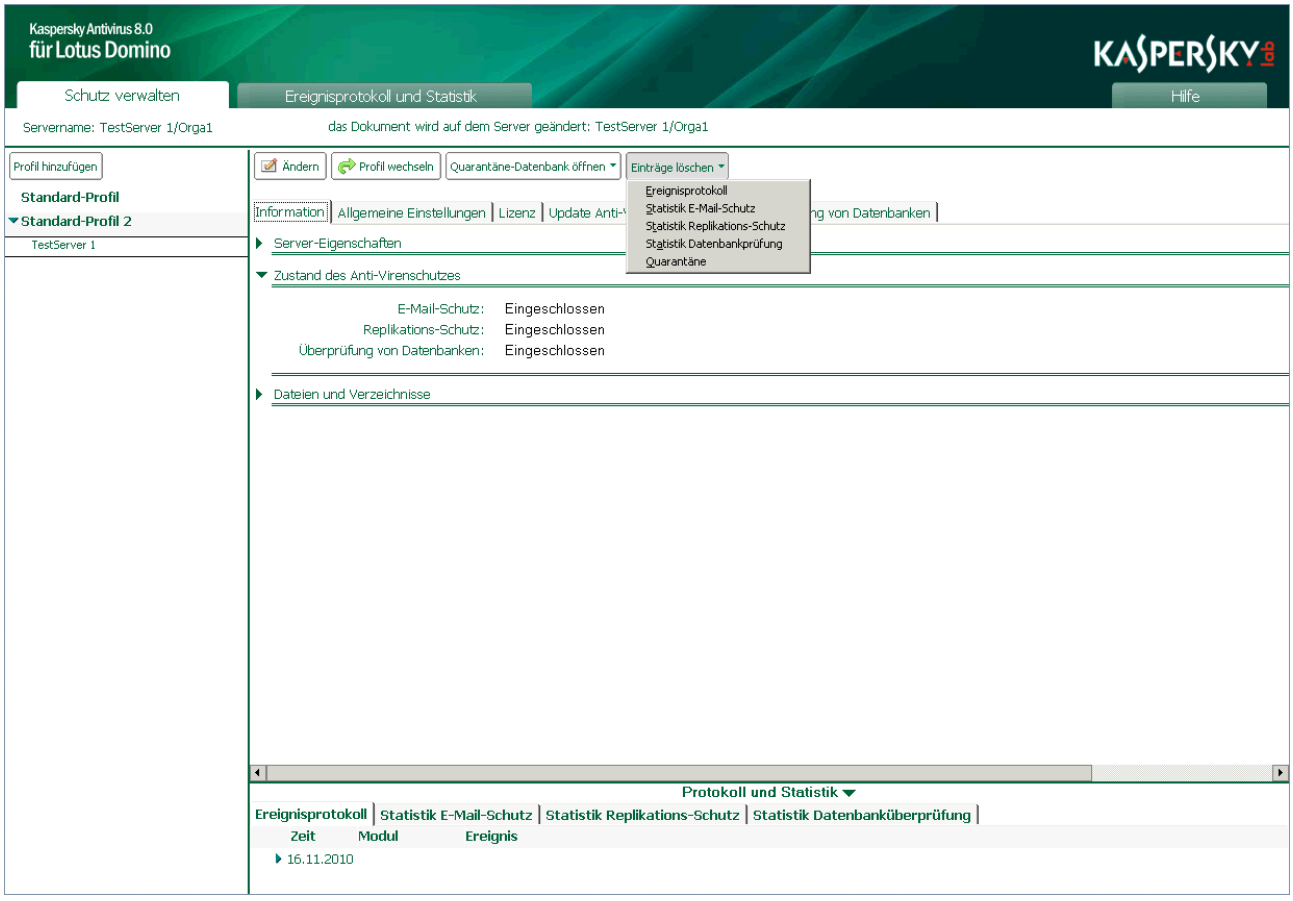


Abbildung 39: Löschen der Einträge aus dem Ereignisprotokoll und der Statistik

3. Betätigen Sie die Schaltfläche **Einträge löschen** im Action panel und wählen die gewünschte Aufgabe aus der Combobox. Die Liste enthält Elemente zum Löschen der folgenden Information:

   - **Ereignisprotokoll**.
   - **Statistik des E-Mail-Schutzes**.
   - **Statistik Replikations-Schutz**.
   - **Statistik Datenbankprüfung**.

Demzufolge werden Informationen die dem von Ihnen ausgewählten Punkt entspricht aus der kaveventslog.nsf Datenbank , gelöscht.

DIE EREIGNISPROTOKOLL- UND STATISTIKDATENBANK EINSEHEN

Kaspersky Anti-Virus ermöglicht es Ihnen die folgenden Information einzusehen, welche in der Ereignisprotokoll- und Statistikdatenbank (kaveventslog.nsf) hinterlegt sind:

- **Ereignisprotokoll**.
- **Statistik des E-Mail-Schutzes**.
- **Statistik Datenbankprüfung**.
- **Statistik Replikations-Schutz**.

Dabei können Sie Information für einen Server (s. Abschnitt "Ereignisprotokoll und Statistik für einen Server einsehen" auf der S. 107), aber auch allgemeine Informationen über alle Server einsehen (s. Abschnitt "Allgemeines Ereignisprotokoll und Statistik durchsehen" auf der S. 105), unabhängig davon, im Bestand welchen Profils sie hinterlegt sind.

IN DIESEM ABSCHNITT

Allgemeines Ereignisprotokoll und Statistik einsehen 105

Ereignisprotokoll und Statistik für einen Server durchsehen 107

ALLGEMEINES EREIGNISPROTOKOLL UND STATISTIK EINSEHEN

Um die allgemeinen Ereignisprotokolle und Statistiken von allen geschützten Servern einzusehen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Ereignisprotokoll und Statistik.**
2. Im Navigation panel wählen Sie den Teil, der die nötigen Informationen enthält: **Ereignisprotokoll**, **Statistik des E-Mail-Schutzes**, **Statistik Datenbankprüfung**, **Statistik Replikations-Schutz**.
3. Im diesem Teil wählen Sie einen der dargestellten Abschnitte.

   Demzufolge werden im Ansichtsbereich Einträge des ausgewählten Abschnitts dargestellt. In den Abschnitten **Allgemein** werden sämtliche Informationen, die in der kaveventslog.nsf Datenbank für den ausgewählten Teil hinterlegt ist, dargestellt. Um die Informationsdurchsicht und -suche zu erleichtern, werden die Einträge in Abschnitten gruppiert.

   Um die komplette Liste der gruppierten Einträge zu öffnen, betätigen Sie . Um die Liste zusammenzuklappen, betätigen Sie .

Dies schließt den Ereignistyp und zusätzliche Informationen darüber mit ein.Die in der Tabelle dargestellten Einträge können Auf- und Absteigend nach **Datum** und **Zeit** dargestellt werden, sowie alphabetisch nach **Servername** und **Modul** sortieret. Um Einträge zu sortieren, drücken Sie das Zeichen links vom Spaltennamen .

EREIGNISPROTOKOLL

Im Teil **Ereignisprotokoll** sind folgende Abschnitte dargestellt:

- **Allgemein** – vollständige Ereignisliste ohne irgendwelche Gruppierungen.
- **Nach Servername** – eine Liste der Ereignisse, die nach Servernamen, auf welche Ereignisse festgestellt wurden, gruppiert sind.
- **Nach Datum** – eine Liste der Ereignisse, die nach Datum und Uhrzeit ihrer Erfassung gruppiert sind.
- **Nach Wichtigkeit** – eine Liste der Ereignisse, die nach dem Wichtigkeitsniveau gruppiert sind (**Kritische Ereignisse**, **Wichtige Ereignisse**, **Informationsereignisse**).

Um die komplette Liste der gruppierten Einträge zu öffnen, betätigen Sie . Um die Liste zusammenzuklappen, betätigen Sie .

Über jedes Ereignis werden folgende Informationen in den Protokollabschnitten aufgeführt:

- Ein Zeichen, das das Wichtigkeitsniveau des Ereignisses darstellt:
  - — *kritisches Ereignis*. Ein Ereignis von kritischer Wichtigkeit, das auf Probleme während des Betriebs von Kaspersky Anti-Virus Arbeit hinweist. Zu solchen Ereignissen werden beispielsweise die Entdeckung einer Bedrohung oder eine Störung im laufenden Betrieb aufgezählt.
  - — *Warnmeldung*. Ein Ereignis, das unbedingt beachtet werden muss, denn es stellt eine Situation im laufenden Betrieb dar, welche ein Eingreifen erfordert, beispielsweise: **Lizenz läuft bald ab**.
  - — *Ereignis mit Informationscharakter.* Ein Ereignis mit Auskunftscharakter, beispielsweise: **Aufgabe erfolgreich gestartet**.
- **Datum** – Datum der Ereigniserfassung.
- **Zeit** – Uhrzeit der Ereigniserfassung.
- **Servername** – Name des Servers, auf dem das Ereignis erfasst wurde.
- **Modul** – Name des Moduls, während der Ereigniserfassung lief.
- **Ereignis** – Beschreibung des erfassten Ereignisses. Dies schließt den Ereignistyp und zusätzliche Informationen darüber mit ein.

Dies schließt den Ereignistyp und zusätzliche Informationen darüber mit ein.Die in der Tabelle dargestellten Einträge können Auf- und Absteigend nach **Datum** und **Zeit** dargestellt werden, sowie alphabetisch nach **Servername** und **Modul** sortieret. Um Einträge zu sortieren, drücken Sie das Zeichen links vom Spaltennamen .

STATISTIK

Im Statistikteil sind folgende Abschnitte dargestellt:

- **Allgemein** – vollständige statistische Informationen des ausgewählten Abschnitts ohne jegliche Gruppierung.
- **Nach Servernamen** – statistische Informationen, die nach Namen der Server, auf welchen die Statistik erstellt wurde, gruppiert ist.
- **Nach Datum** – statistische Informationen, die nach Datum und Uhrzeit ihrer Erfassung gruppiert sind.
- **Nach Objektstatus** – statistische Informationen, die nach dem Objektstatus gruppiert sind.
- **Nach Absendernamen** – statistische Informationen, die nach Adressen der E-Mail-Absender gruppiert sind (nur für die Statistik des E-Mail-Schutzes).

- **Nach Datenbankname** – statistische Information, die nach den Datenbanknamen, in welchen infizierte Dokumente entdeckt wurden, gruppiert sind (nur für die Statistik des Replikationsschutzes und der Datenbankenuntersuchung).
- **Nach Autor der letzten Änderungen** – statistische Informationen, die nach Namen der Verfasser der letzten Änderungen im Dokument gruppiert sind (nur für die Statistik des Replikationsschutzes und der Datenbankenuntersuchung).

Um die komplette Liste der gruppierten Einträge zu öffnen, betätigen Sie . Um die Liste zusammenzuklappen, betätigen .

Über jedes Ereignis werden in den Statistikteilen folgende Information aufgeführt:

- ein Zeichen, das den Status des untersuchten Objekts darstellt:
  - – das Objekt wurde behandelt;
  - – das Objekt ist nicht desinfizierbar;
  - – das Objekt wurde nicht überprüft;
  - – das Objekt ist möglicherweise infiziert.
- **Datum** – Datum der Objektuntersuchung.
- **Zeit** – Uhrzeit der Objektuntersuchung.
- **Servername** – Name des Servers, auf dem die Untersuchung ausgeführt wurde.
- **Absender** – die E-Mail-Adresse des Absenders der E-Mail, in der das Objekt entdeckt wurde (nur für die Statistik des E-Mail-Schutzes).
- **Empfänger** – E-Mail-Adresse des Empfängers der E-Mail, in der das Objekt entdeckt wurde (nur für die Statistik des E-Mail-Schutzes).
- **Datenbankname** – Name der Datenbank, in der sich das untersuchte Objekt befindet (nur für die Statistik des Replikationsschutzes und der Datenbankenuntersuchung).
- **Modul** – Name des Moduls, welches das Objekt untersucht hat.
- **Bedrohung** – Name der Bedrohung, falls das untersuchte Objekt infiziert ist. Falls das Objekt nicht infiziert ist, wird sein Name und Status, der nach den Ergebnissen der Anti-Viren-Untersuchung ermittelt wird, angegeben.
- **Autor Änderungen** – Name des Benutzers, der die letzte Änderung ins Dokument eingetragen hat und der Name des Servers, auf dem die Änderungen am Dokument durchgeführt wurden. Format: **<Benutzername/Servername>** (nur für die Statistik des Replikationsschutzes und der Datenbankenuntersuchung).

Einträge in der Tabelle können Auf- und Absteigend nach **Datum** und **Zeit** Spalten, dargestellt sind, sowie alphabetisch für die in den **Servername** und **Modul** Spalten dargestellten Werte, sortieren. Um Einträge zu sortieren, drücken Sie das Zeichen links vom Spaltennamen.

EREIGNISPROTOKOLL UND STATISTIK FÜR EINEN SERVER DURCHSEHEN

Um das Ereignisprotokoll und die Statistik für einen Server einzusehen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Wählen Sie im Profilbestand des Navigation panels den Server, dessen Informationen Sie einsehen wollen.

Einträge der Ereignisprotokoll- und Statistikdatenbank sind im Ansichtsbereich folgender Tabs dargestellt: **Ereignisprotokoll**, **Statistik des E-Mail-Schutzes**, **Statistik Replikations-Schutz**, **Statistik Datenbanküberprüfung**.

Im ausgewählten Tab wird dieselbe Information dargestellt wie auch im allgemeinen Ereignisprotokoll (s. Abschnitt "Ereignisprotokoll" auf der S. 105) und in der allgemeinen Statistik (s. Abschnitt "Statistik" auf der S. 106).

Die Einträge in allen Tabs sind nach dem Erfassungszeitraum gruppiert. Die Statistik des E-Mail-Schutzes ist zusätzlich noch nach den E-Mail-Adressen der Absender gruppiert. Die Statistik des Replikationsschutzes und der Datenbankenuntersuchung, sind nach den Namen der Datenbanken, in welchen sich die untersuchten Dokumente befinden gruppiert. Um die ganze Liste zu öffnen, betätigen Sie . Um die Liste zusammenzuklappen, betätigen .

BENACHRICHTIGUNGEN

Kaspersky Anti-Virus ermöglicht es Ihnen über folgende Objekte, die bei der Untersuchung von E-Mails, Replikationen und Datenbanken entdeckten wurden, benachrichtigt zu werden:

- **Nicht desinfizierbares Objekt**.
- **Desinfizierbares Objekt**.
- **Möglicherweise infiziertes Objekt**.
- **Nicht geprüftes Objekt**.

Falls bei der Untersuchung der E-Mails eine Anhäufung von infizierten, möglicherweise infizierten, beschädigten Objekten und Objekten, welche eine gleichartige Bedrohung enthalten, festgestellt wurde, benachrichtigt Kaspersky Anti-Virus die Administratoren über eine drohende Epidemie (s. Abschnitt "Benachrichtigungen über Epidemien" auf der S. 68). Die Kriterien, nach welchen eine Benachrichtigung über eine Epidemie versandt wird, werden vom Administrator für jede einzelne Objektkategorie separat eingegeben.

Die Benachrichtigung kann auch Informationen über ausgeführte Aktionen und Ergebnisse der Objektverarbeitung enthalten.

Bei der Untersuchung der E-Mails kann die Information zum Body der untersuchten E-Mail hinzugefügt werden. Absender, Empfänger, Server- und Profiladministratoren, können die Benachrichtigungsmeldungen per E-Mail empfangen.

Bei der Untersuchung der Replikationen und Datenbanken können die Benachrichtigungsmeldungen an Serveradministratoren und Administratoren des Profils, zu welchem dieser Server gehört, gesendet werden. Muster von Benachrichtigungsmeldungen werden in den Einstellungen des Replikationsschutzes und der Datenbankenuntersuchung angegeben.

Serveradministratoren werden in den Servereinstellungen angegeben (s. Abschnitt "Einsetzung vom Serveradministrator" auf der S. 114): Im Tab **Information** im Bereich **Server-Eigenschaften**. Die Profiladministratoren werden in den Profileinstellungen angegeben (s. Abschnitt "Einsetzung vom Profiladministrator" auf der S. 114): Im Tab **Allgemeine Einstellungen** im Bereich **Sicherheit**.

Die Einstellungen der Benachrichtigungen über entdeckte nicht desinfizierbare, desinfizierbare, möglicherweise infizierte und nicht untersuchte Objekte werden separat für jeden einzelnen Status in den Einstellungen des E-Mail-, Replikationsschutzes und der Datenbankenuntersuchung angegeben.

Die Benachrichtigungseinstellungen werden vom Profil, zu welchem der geschützte Server gehört, vorgegeben. Die Anpassung der einzelnen Einstellungen der Benachrichtigung für einen Server ist nicht vorgesehen.

Um die Benachrichtigungseinstellungen bei Epidemien anzupassen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, dessen Einstellungen Sie ändern möchten.

3. Betätigen Sie die Schaltfläche **Ändern** im Action panel, und wählen im Verwaltungsbereich im Tab **E-Mail-Schutz / Replikations-Schutz / Überprüfung von Datenbanken**, den Tab **Aktionen** (s. Abbildung unten).

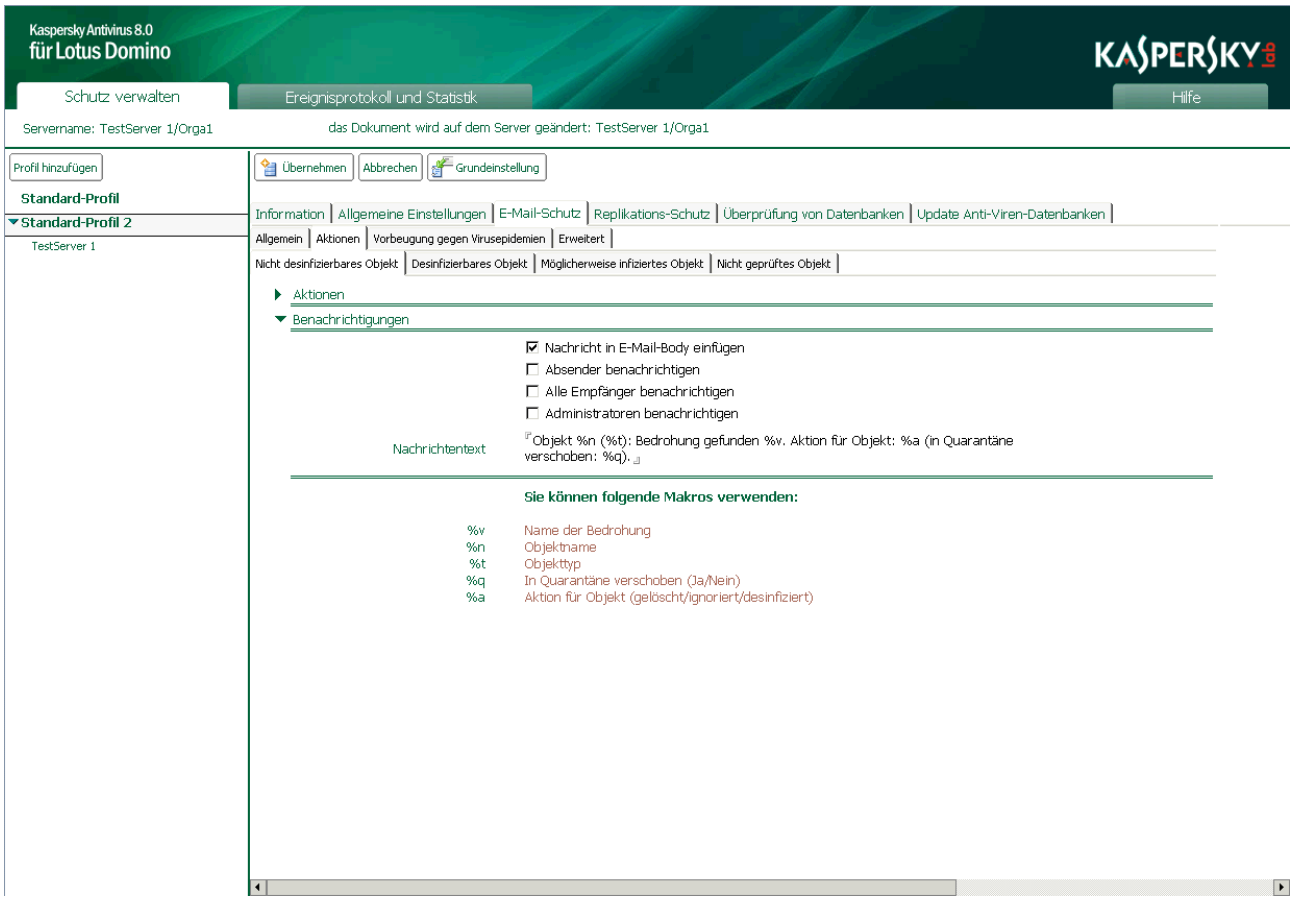


Abbildung 40: Anpassung der Einstellungen der der Benachrichtigungen

4. Im Tab **Aktionen** wählen Sie den Tab, der dem Status der Objekte entspricht,für welchen Sie die Benachrichtigungen anpassen möchten. Sie können aus folgenden Tabs wählen

   - **Nicht desinfizierbares Objekt** – Einstellungsanpassung der Benachrichtigungen über infizierte nicht desinfizierbare Objekte.

   - **Desinfizierbares Objekt** – Einstellungsanpassung der Benachrichtigungen über infizierte desinfizierbare Objekte.

   - **Möglicherweise infiziertes Objekt** – Einstellungsanpassung der Benachrichtigungen über möglicherweise infizierte Objekte.

   - **Nicht geprüftes Objekt** – Einstellungsanpassung der Benachrichtigungen über nicht untersuchte Objekte.

5. Im **Benachrichtigungen** Bereich (s. Abbildung oben) passen Sie die Einstellungen an, nach welchen Benachrichtigungen über entdeckte Objekte und ausgeführte Aktionen versendet werden. Dazu setzen bzw. entfernen Sie folgende Häkchen:

   - **Nachricht in E-Mail-body einfügen** – zum Body der Ursprungsmail wird eine Informationsmeldung, die nach dem im **Nachrichtentext** Feld vorgegebenen Muster erstellt wurde, hinzugefügt.

   - **Absender benachrichtigen** – eine Benachrichtigungsmeldung, die nach dem im **Nachrichtentext** Feld eingegebenen Muster erstellt wurde, per E-Mail an die Absenderadresse senden.

   - **Absender benachrichtigen** – eine Benachrichtigungsmeldung, die nach dem im **Nachrichtentext** Feld eingegebenen Muster erstellt wurde, per E-Mail an die Absenderadresse senden.

- **Administratoren benachrichtigen** – eine Benachrichtigungsmeldung, die nach dem im **Nachrichtentext** Feld eingegebenen Muster erstellt wurde, per E-Mail an die Adresse der Serveradministratoren und entsprechenden Profiladministratoren, senden.

  Serveradministratoren werden in den Servereinstellungen angegeben (s. Abschnitt "Einsetzung vom Serveradministrator" auf der S. 114): Im Tab **Information** im Bereich **Server-Eigenschaften**. Die Profiladministratoren werden in den Profileinstellungen angegeben (s. Abschnitt "Einsatz eines vom Profiladministrators" auf der S. 114): Im Tab **Allgemeine Einstellungen** im Bereich **Sicherheit**.

Im Feld **Nachrichtentext** erstellen Sie den Text, der als Benachrichtigung hinzugefügt werden soll. Sie können folgende Makros verwenden:

- **%v** – Name der im Objekt entdeckten Bedrohung;
- **%n** – Name des Objekts, in dem die Bedrohung entdeckt wurde;
- **%t** – Typ des Objekts, in dem die Bedrohung entdeckt wurde: E-Mail-Body, Anhang, OLE-Objekt;
- **%q** – Informationen über die Speicherung von Objektkopien in die Quarantäne Datenbank: **ja** – das Objekt wurde in die Quarantäne verschoben, **nein** – das Objekt wurde nicht in die Quarantäne verschoben;
- **%d** – Informationen über die Löschung eines Objekts: **ja** – das Objekt wurde gelöscht, **nein** – das Objekt wurde nicht gelöscht.

6. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Um die standardmäßigen Einstellungswerte wiederherzustellen, betätigen Sie die Schaltfläche **Grundeinstellung**.

KONFIGURATIONSVERWALTUNG

Die Einstellungen des Betriebs von Kaspersky Anti-Virus werden von den Profil- und Servereinstellungen bestimmt (s. Abschnitt "Kaspersky Anti-Virus Einstellungsverwaltung" auf der S. 26).

Durch ein Profil kann man einheitliche Kaspersky Anti-Virus Einstellungen für eine Server-Gruppe vorgeben, sowie ein Schutzsystem mit verschiedenen Sicherheitsniveaus erstellen. Durch die Servereinstellungen kann man einige Einstellungen für jeden einzelnen Server neu angeben, den Serverfunktionen im Netzwerk entsprechend.

Sie können Profile erstellen und löschen, Server zu einem anderen Profil verschieben oder die Profil- und Servereinstellungswerte ändern.

Vor der Ausführung der nötigen Operationen (Profil erstellen und löschen, Servereinstellungen anpassen, usw.) überzeugen Sie sich bitte davon, dass das Benutzerkonto, unter welchem die Verwaltungscenter Datenbank geöffnet wird, über genügend Berechtigungen zum Ausführen dieser Operationen verfügt.

IN DIESEM ABSCHNITT

Profile erstellen und löschen 112

Einsetzung vom Profiladministrator 114

Einsetzung vom Serveradministrator 114

Server zu einem anderen Profil verschieben 115

Anpassung der einzelnen ServerEinstellungswerte 115

Verwendung der Option der direkten Bearbeitung der Servereinstellungen 118

PROFILE ERSTELLEN UND LÖSCHEN

Über Rechte zur Erstellung und Entfernung von Profilen–, verfügen nur die Benutzer, welche Berechtigungen der Funktionsgruppen **Sicherheitsadministratoren** und **ControlCenter-Administratoren** besitzen.

Um ein Profil zu erstellen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel betätigen Sie die Schaltfläche **Profil hinzufügen**.

   Demzufolge werden im Verwaltungsbereich die Einstellungen des neuen Profils dargestellt. Standardmäßig wird das Profil mit den Einstellungswerten, die von Kaspersky Lab Spezialisten empfohlen wurden, erstellt. Sie können die Profileinstellungen anpassen.

3. Im Verwaltungsbereich im Tab **Information** im Feld **Profilname** geben Sie den Profilnamen an. Der Profilname darf noch nicht vergeben sein (s. Abbildung unten).

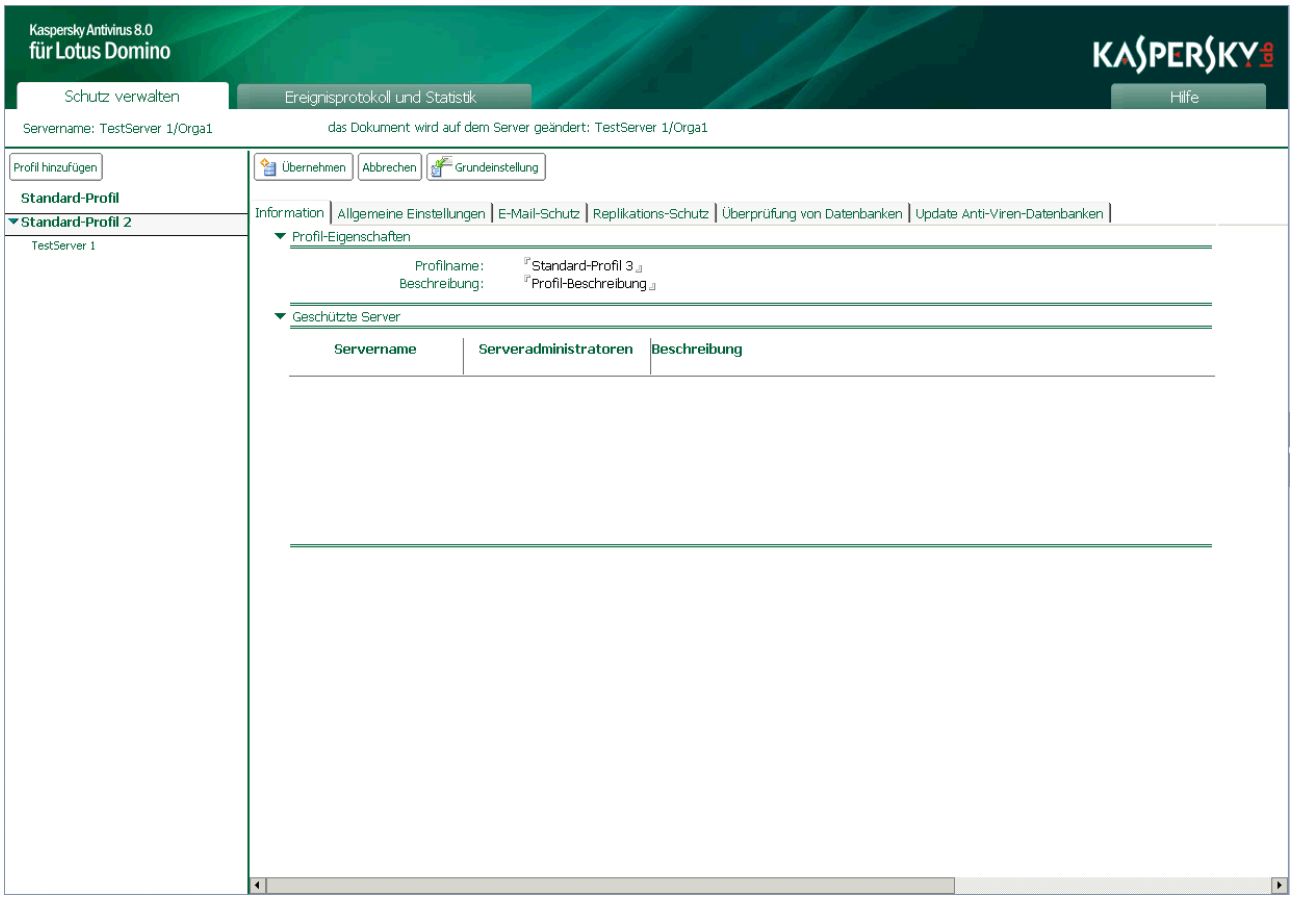


Abbildung 41: Anpassung der Profileinstellungen

4. Im Feld **Beschreibung** geben Sie zusätzliche Informationen über das Profil an.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

   Demzufolge wird die Information über das Profil zum Replikat der Verwaltungscenter Datenbank hinzugefügt, welche sich auf dem Server befindet, auf dem die Datenbank geöffnet wurde. Bei der nächsten Replikation werden die Einstellungsänderungen an andere geschützte Server weitergegeben.

Um ein Profil zu erstellen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie das Profil, welches Sie löschen wollen.

   Vor dem Löschen des Profils müssen alle Server aus seinem Bestand verschoben werden.

3. Betätigen Sie die Schaltfläche **Löschen** im Action panel.

   Demzufolge wird die Information über das Profil zum Replikat der Verwaltungscenter Datenbank hinzugefügt, welche sich auf dem Server befindet, auf dem die Datenbank geöffnet wurde. Bei der nächsten Replikation werden diese Änderungen an andere geschützten Server weitergegeben.

Sie können das Profil auch mit dem Punkt **Löschen** aus dem Profilkontextmenü oder mit der **Delete** Taste löschen. In diesem Fall wird faktisches Löschen vom Profil beim Abschluss der Verwaltungscenter Datenbank beim Drücken auf der **F9** Taste vollgezogen.

EINSETZUNG VOM PROFILADMINISTRATOR

Um den Profiladministrator einzusetzen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie das Profil, für das Sie den Administrator einsetzen wollen.
3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und,wählen den Tab **Allgemeine Einstellungen** aus dem Verwaltungsbereich.
4. Im **Sicherheit** Bereich geben Sie den Namen vom Profiladministrator oder den Namen der Administratorengruppe auf eine der folgenden Weisen ein:
   - Geben Sie den Administratornamen oder den Namen der Administratorengruppe manuell an. Das Format der Eintragung des Administratornamens ist hierarchisch (Hierarchie Notes, Hierarchie der Organisation).
   - Wählen Sie den Administratornamen oder den Namen der Administratorengruppe aus dem Adressbuch des Domino-Servers. Dazu bestätigen Sie .

   Als Profiladministrator kann nur der Benutzer eingesetzt werden, der Berechtigungen einer der drei Funktionsgruppen besitzt: **Sicherheitsadministratoren**, **ControlCenter-Administratoren** oder **Administratoren mit eingeschränkten Berechtigungen**.

   Standardmäßig werden als Profiladministratoren die Benutzer angegeben, die bei der Programminstallation in die **ControlCenter-Administratoren** Gruppe eingeschlossen wurden.
5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern. Sie können standardmäßige Parameterwerte mit die Schaltfläche **Grundeinstellung** wiederherstellen.

EINSETZUNG VOM SERVERADMINISTRATOR

Um den Profiladministrator einzusetzen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie im Profilbestand den Server aus dem Profilbestand, für den Sie den Administrator einsetzen wollen.
3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und wählen den Tab **Information** aus dem Verwaltungsbereich.
4. Im Bereich **Server-Eigenschaften** geben Sie den Namen des Serveradministrators oder den Namen der Administratorengruppe auf eine der folgenden Weisen an:
   - Geben Sie den Administratornamen oder den Namen der Administratorengruppe manuell an. Das Format der Eintragung des Administratornamens ist hierarchisch (Hierarchie Notes, Hierarchie der Organisation).
   - Wählen Sie den Administratornamen oder den Namen der Administratorengruppe aus dem Adressbuch des Domino-Servers. Dazu bestätigen Sie .

Als Serveradministrator kann nur ein Benutzer bestimmt werden, welcher über die Berechtigungen einer der drei Funktionsgruppen verfügt: **Sicherheitsadministratoren**, **ControlCenter-Administratoren** oder **Administratoren mit eingeschränkten Berechtigungen**).

Standardmäßig werden als Serveradministratoren die Benutzer angegeben, die bei der Programminstallation in die **ControlCenter-Administratoren** Gruppe aufgenommen wurden.

5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

SERVER ZU EINEM ANDEREN PROFIL VERSCHIEBEN

Um einen Server von einem zum anderen Profil zu verschieben, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie ein Profil, wenn Sie die Statistikeinstellungen für eine Server-Gruppe anpassen möchten oder den Server, wenn Sie die Statistikeinstellungen für einen einzelnen Server anpassen möchten.
3. Im Action panel betätigen Sie die Schaltfläche **Profil wechseln**.
4. Im geöffneten Fenster **Wechsel des Profils** wählen Sie das Profil aus der Liste, zu dessen Bestand Sie den Server verschieben möchten, und betätigen die Schaltfläche **OK**.

   Demzufolge wird der ausgewählte Server zu einem anderen Profilbestand verschoben. Bei der nächsten Replikation werden diese Änderungen an andere geschützten Server weitergegeben.

   Falls in den Servereinstellungen das Häkchen bei **Profil-Einstellungen verwenden** gesetzt ist, werden nach dem Verschieben die Einstellungswerte des neuen Profils für den Server verwendet. Falls das Häkchen bei **Profil-Einstellungen verwenden** nicht gesetzt ist, werden für alle Servereinstellungen ihre derzeitigen Werte benutzt.

ANPASSUNG DER EINZELNEN SERVEREINSTELLUNGSWERTE

Standardmäßig verwendet der geschützte Server die Einstellungen des Profils, in dessen Bestand er aufgenommen wurde. Sie können einige vom Profil vorgegebene Einstellungen erneut angeben, indem Sie die einzelne Servereinstellungswerte anpassen.

Sie können folgende Einstellungen erneut angeben:

- Update-Einstellungen:
  - Updatequelle der Anti-Viren-Datenbanken.
  - Verbindungseinstellungen zur Updatequelle.
  - Update-Zeitplan.
- Einstellungen des Ereignisprotokolls und der Statistik:
  - Detaillierungsgrad der im Protokoll festgestellten Informationen.
  - Aufbewahrungsort der Informationen über erfasste Ereignisse.

- Aufbewahrungsfrist der Einträge des Ereignisprotokolls.
- Aufbewahrungsfrist der statistischen Informationen.

Um einzelne Einstellungswerte für das Serverupdate anzugeben, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie ein Profil, wenn Sie die Statistikeinstellungen für eine Server-Gruppe anpassen möchten oder den Server, wenn Sie die Statistikeinstellungen für einen einzelnen Server anpassen möchten.
3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und wählen den Tab **Update Anti-Viren-Datenbanken** im Verwaltungsbereich.
4. Im Bereich **Update-Einstellungen** entfernen Sie das Häkchen bei **Profil-Einstellungen verwenden** (s. Abbildung unten).

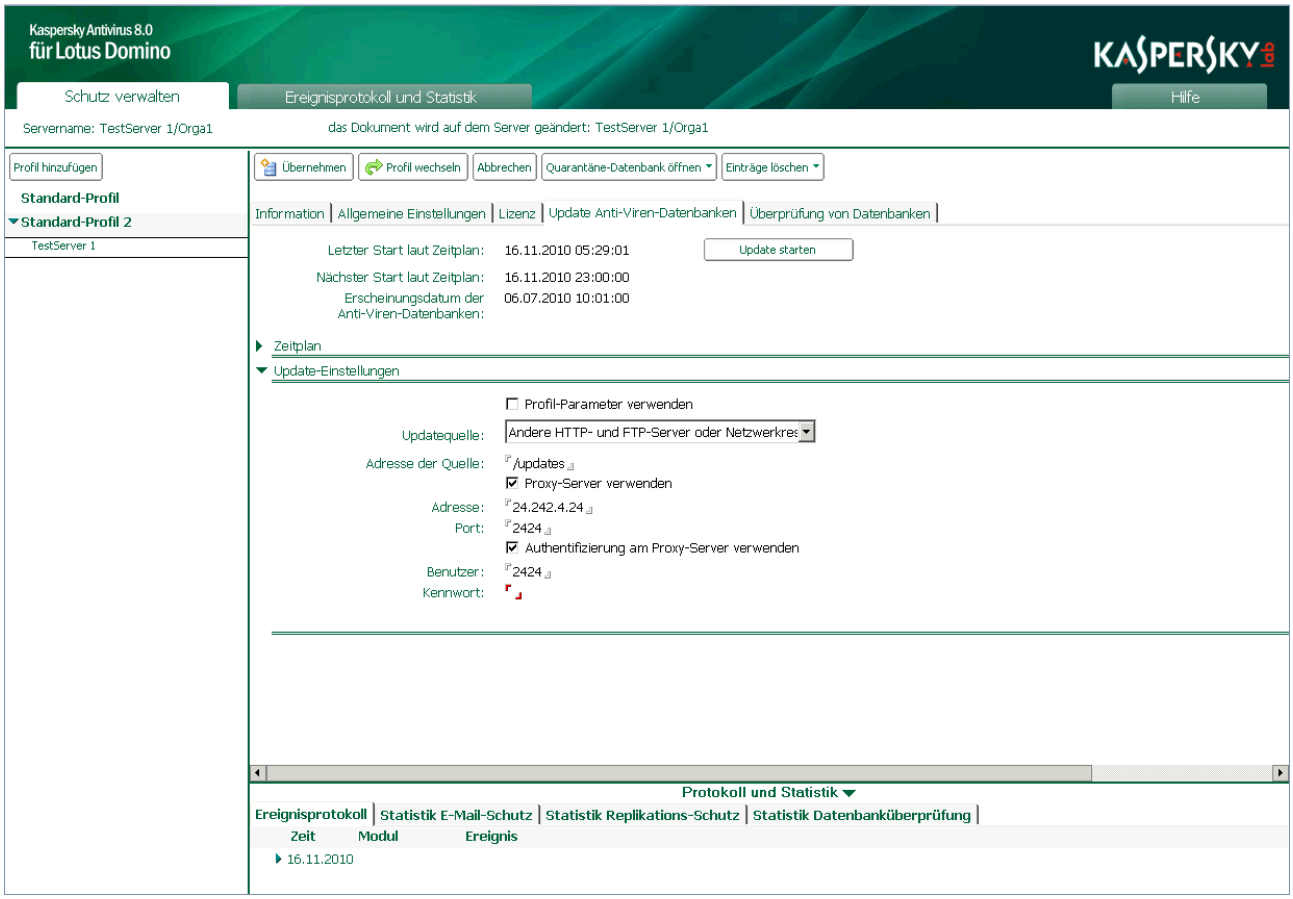


Abbildung 42: Anpassung der einzelnen Update-Einstellungen für einen Server

Falls das Häkchen gesetzt ist, können die Update-Einstellungen nicht geändert werden.

5. Geben Sie für den entsprechenden Server die Einstellungen des Anti-Viren-Datenbanken-Updates (s. Abschnitt "Updatequelle auswählen" auf der S. 55) an oder legen Sie den Zeitplan fest (s. Abschnitt "Planmäßiges Update" auf der S. 56).
6. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

Um einzelne Parameterwerte von Ereignisprotokoll und Statistik für einen Server einzustellen, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.

2. Im Navigation panel wählen Sie im Profilbestand den Server, für den Sie einzelne Parameterwerte eingeben wollen.

3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und wählen Sie den Tab **Allgemeine Einstellungen** aus dem Verwaltungsbereich.

4. Im Bereich **Protokolleinstellungen** entfernen Sie das Häkchen bei **Profil-Einstellungen verwenden** (s. Abbildung unten).

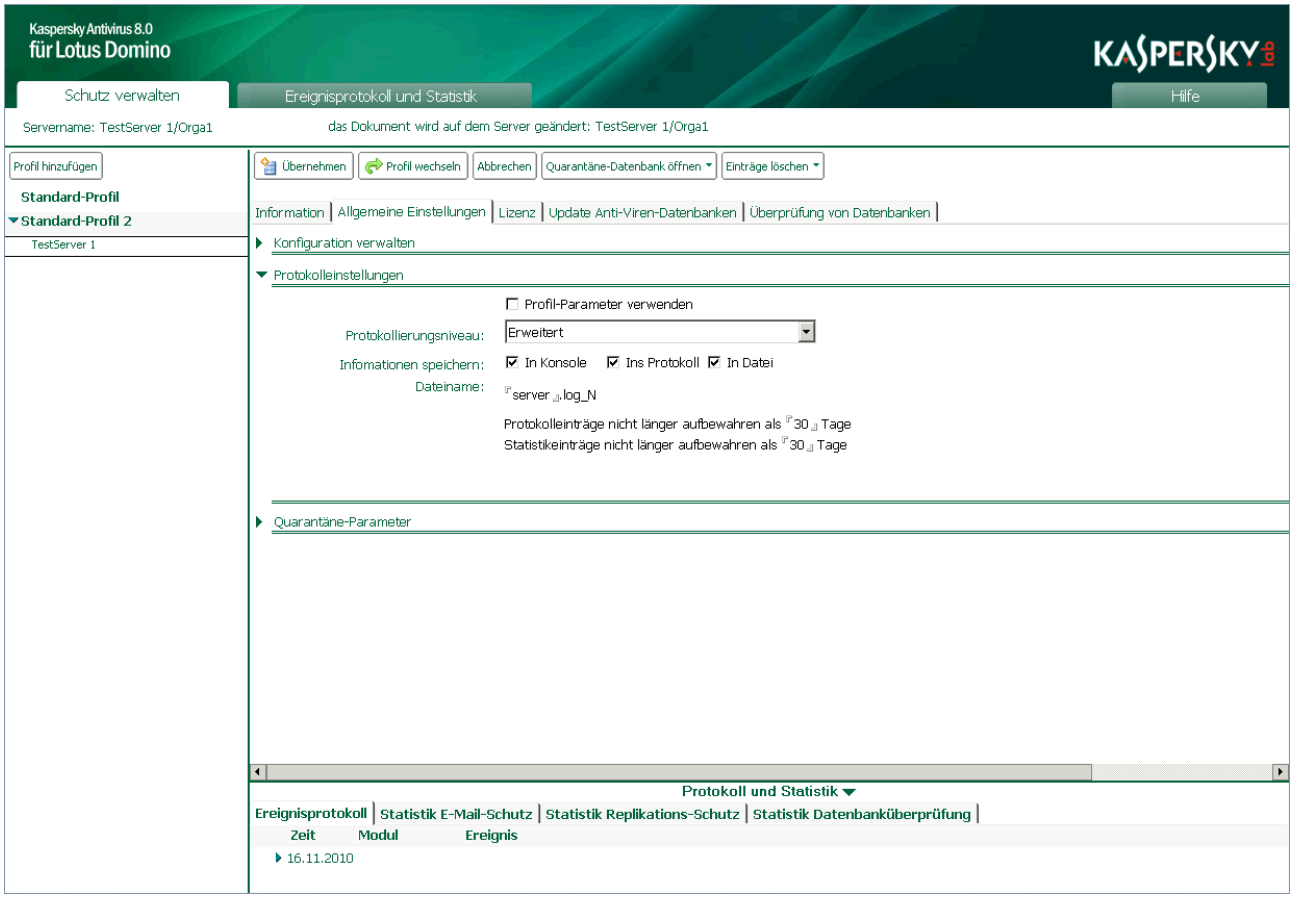


Abbildung 43: Anpassung der einzelnen Einstellungswerte des Ereignisprotokolls und der Statistik für einen Server

5. Passen Sie die Einstellungen des Ereignisprotokolls (s. Abschnitt "Einstellungen des Ereignisprotokolls" auf der S. 99) oder die Statistikeinstellungen an (s. Abschnitt "Statistikeinstellungen" auf der S. 101).

6. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

VERWENDUNG DER OPTION DER DIREKTEN BEARBEITUNG DER SERVEREINSTELLUNGEN

Standardmäßig werden die Änderungen der Servereinstellungen in das Datenbankreplikat auf dem Server, mit dem die Verbindung besteht, eingetragen. Falls Sie die Servereinstellungen via Lotus Notes Client anpassen, werden die Änderungen in das Replikat der Verwaltungscenterdatenbankeingetragen, welche sich auf dem Server befindet, dessen Einstellungen Sie bearbeiten. Dies geschieht unabhängig davon, mit welchen Server Sie verbunden sind. In diesem Fall werden die neue Einstellungswerte auf dem geschützten Server wesentlich schneller verwendet. Bei der Arbeit via Web-Browser werden die Änderungen der Servereinstellungen immer in das Datenbankreplikat eingetragen, welche sich auf dem Server befindet, mit welchem Sie verbunden sind.

Um die Änderungen der Servereinstellungen in das Replikat der Verwaltungscenterdatenbank des Servers einzutragen den Sie bearbeiten, gehen Sie wie folgt vor:

1. Im Switch panel wählen Sie den Tab **Schutz verwalten**.
2. Im Navigation panel wählen Sie den Server aus dem Profilbestand, dessen Einstellungen Sie anpassen möchten.
3. Im Action panel betätigen Sie die Schaltfläche **Ändern** und,wählen den Tab **Allgemeine Einstellungen** aus dem Verwaltungsbereich.
4. Setzen Sie das Häkchen bei **Dokument auf dem geschützten Server ändern** im Bereich **Konfiguration verwalten**.
5. Betätigen Sie die Schaltfläche **Übernehmen**, um die durchgeführten Änderungen zu speichern.

ÜBERPRÜFUNG DER PROGRAMMEINSTELLUNGEN AUF RICHTIGKEIT

IN DIESEM ABSCHNITT

Test "virus" EICAR und seine Modifikationen 119

Testen des E-Mail-Schutzes 120

Testen des Replikationsschutzes 121

Testen der Datenbankenuntersuchung 121

TEST "VIRUS" EICAR UND SEINE MODIFIKATIONEN

Der Test-"virus" wurde von der EICAR Organisation (The European Institute for Computer Antivirus Research) eingens zum Test von Anti-Viren-Produkten entwickelt.

Der Test-"virus" an sich IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Computer schädigen kann, dennoch wird er von den meisten Hersteller als bösartiges Programm erkannt.

Verwenden Sie keine echte Viren um die Funktionsfähigkeit von Anti-Viren-Produkten zu testen!

Der Test-"virus" kann auf der offiziellen Web-Seite der **EICAR** Organisation heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Vor dem Herunterladen sollte das auf Ihrem Computer installierte Anti-Viren-Programm deaktiviert werden, da die *anti_virus_test_file.htm* Datei als ein via HTTP-Protokoll übertragenes infiziertes Objekt erkannt wird.

Vergessen Sie nicht, den Anti-Viren-Schutz umgehend nach dem Herunterladen des Test-"viruses" wieder zu aktivieren!

Das Programm erkennt die von der **EICAR** Web-Seite heruntergeladene Datei als infiziertes Objekt, welches einen nicht desinfizierbaren "Virus" enthält, und führt die Aktion aus, die für ein solches Objekt vorgesehen ist.

Sie können auch Modifikationen des Standardtest-"viruses" zum Test der Kaspersky Anti-Virus Funktionsfähigkeit verwenden. Dafür müssen Sie den Inhalt des Standard-"virusese" ändern, indem Sie einen der Präfixe hinzufügen (s. Tabelle weiter). Zum Erstellen einer Test-"virus"-Modifikation kann ein beliebiger Text- oder Hypertexteditor, beispielsweise, **Microsoft Notepad**, **VIM UltraEdit32**, usw. verwendet werden.

Sie können die Korrektheit des AntiViren-Programmablaufs mit dem modifizierten EICAR-Virus nur prüfen, wenn die eingesetzten Anti-Virendatenbanken nicht älter als jene vom 24.10.03 sind (Kumulatives Update – Oktober, 2003).

In der ersten Spalte werden Präfixe angegeben, die am Zeilenanfang des Standardtest-"viruses" hinzugefügt werden. In der zweiten Spalte sind alle möglichen Werte des Status, der dem Objekt nach den Ergebnissen der Anti-Viren-Untersuchung von Kaspersky Anti-Virus zugewiesen wurde, aufgezählt. Die dritte Spalte enthält Information über die vom Programm ausgeführte Verarbeitung der Objekte mit dem angegebenen Status. Beachten Sie, dass die Aktionen welche an den Objekten von Kaspersky Anti-Virus ausgeführt werden, von den Einstellungswerten bestimmt werden.

Nach dem Hinzufügen eines Präfixes zum Test-"virus" speichern Sie die Datei, beispielsweise, unter dem Namen *eicar_dele.com*. Vergeben Sie ähnliche Namen für alle modifizierten "Viren".Tabelle 1.

Tabelle 6. Modifikationen vom Testvirus

PRÄFIX	OBJEKTSTATUS	INFORMATION ÜBER OBJEKTVERARBEITUNG
das Präfix fehlt, Standardtest-"virus".	**Nicht desinfizierbar**. Das Objekt enthält den Code eines bekannten Virus. Die Behandlung ist nicht möglich.	Kaspersky Anti-Virus erkennt dieses Objekt als nicht desinfizierbaren "Virus" an und führt die Aktion aus, die für nicht desinfizierbare Objekte vorgesehen ist.
CORR-	**Beschädigt**.	Kaspersky Anti-Virus hat Zugriff auf das Objekt erhalten, jedoch ist es ihm nicht gelungen dieses zu untersuchen, da das Objekt beschädigt ist (beispielsweise, Objektstruktur ist verletzt, falsches Dateiformat).
WARN-	**Verdächtig**. Das Objekt enthält den Code eines unbekannten Viruses. Die Behandlung ist nicht möglich.	Das Objekt wurde unter Verwendung des heuristischen Analysators als verdächtige erkannt. Zum Zeitpunkt der Erkennung enthalten die Kaspersky Anti-Virus Datenbanken keine Beschreibung für den Behandlungsvorgang dieses Objekt.
	Verdächtig. Das Objekt enthält den modifizierten Code eines bekannten Viruses. Die Behandlung ist nicht möglich.	Kaspersky Anti-Virus hat eine Teilübereinstimmung eines Codestücks des Objekts mit dem eines bekannten Viruses erkannt. Zum Zeitpunkt der Entdeckung enthalten die Programm-Datenbanken keine Beschreibung für den Behandlungsvorgang für dieses Objekt.
ERRO-	**Untersuchungsfehler**. Bei der Objektuntersuchung ist ein Fehler aufgetreten.	Kaspersky Anti-Virus ist es nicht gelungen, den Zugriff auf das Objekt zu erhalten: Die Vollständigkeit des Objekts ist verletzt (beispielsweise, das Ende des mehrteiligen Archivs fehlt) oder es gibt keine Verbindung mit ihm.
CURE-	**Desinfizierbar**. Das Objekt enthält den Code eines bekannten Virus. Es ist desinfizierbar.	Das Objekt enthält den Virus der behandelt werden kann. Kaspersky Anti-Virus führt die Objektbehandlung aus, dabei wird der Text des "Viren"-Körpers durch CURE ersetzt.

TESTEN DES E-MAIL-SCHUTZES

Für die Überprüfung der Virenerkennung in den E-Mails können Sie ein beliebiges E-Mail-System, welches vom geschützten Domino-Server verwendet wird, gebrauchen. Es wird empfohlen den E-Mailbody und die Anhänge durch Kaspersky Anti-Virus überprüfen zu lassen. Für die Überprüfung der Virenerkennung im E-Mailbody, platzieren Sie den Text des standardisierten oder modifizierten Test-"viruses" in den E-Mailbody.

➧ *Um die Virenerkennung in einer E-Mail-Meldung zu überprüfen, gehen Sie wie folgt vor:*

1. Erstellen Sie eine Meldung im **Klartext Format**.
2. Fügen Sie den Text eines Standard- bzw. eines modifizierten Virus am Anfang der Nachricht ein, und fügen Sie der Nachricht die Datei und das OLE-Objekt bei, die den Test-"viruses" enthalten.
3. Senden Sie die E-Mail an eine beliebige Adresse. Beispielsweise an die Adresse des Serveradministrators oder des Profiladministrators, in dessen Bestand dieser Server enthalten ist.
4. Machen Sie sich mit dem Inhalt der E-Mail, welche an der angegebene Adresse eingegangen ist, vertraut.

Kaspersky Anti-Virus entdeckt das Objekt, erkennt es als nicht desinfizierbar und und führt die Aktion aus, die in den Einstellungen des E-Mail-Schutzes für ein solches Objekt ausgewählt ist. (Im Fall der Verwendung eines modifizierten "Viruses" – dem Präfix entsprechend. Siehe Abschnitt: "Test "virus" EICAR und seine Modifikationen" auf der S. 119), Standardmäßig wird ein nicht desinfizierbares Objekt aus der E-Mail gelöscht. Standardmäßig wird ein nicht desinfizierbares Objekt aus der E-Mail gelöscht.

TESTEN DES REPLIKATIONSSCHUTZES

Es wird empfohlen, die Virenerkennung in Rich Text Format Texten, Anhängen und OLE-Objekten zu überprüfen.

- *Um die Virenerkennung während einer Replikation zu überprüfen, gehen Sie wie folgt vor:*

1. Wählen Sie einen Server auf dem geschützten Server, für welchen die Replikation des konfiguriert ist.

2. Auf dem Server wählen Sie die Datenbank, dessen Replikat sich auf dem geschützten Server befindet. Weiterhin wählen Sie ein Dokument, welches ein RTF-Feld enthält, oder erstellen auf einem nicht geschützten Server eine Datenbank anhand einer der vorhandenen Schablonen und erstellen auf dem geschützten Server ein Replikat dieser Datenbank. In der Datenbank auf dem nicht geschützten Server erstellen Sie ein Dokument, das ein RTF-Feld enthält.

3. Platzieren Sie den Text des standardisierten oder modifizierten Test-"viruses" in das RTF-Feld des ausgewählten Dokuments.

4. Fügen Sie zum ausgewählten Dokument eine Datei oder ein OLE-Objekt hinzu, die den Text des standardisierten oder modifizierten Test-"viruses" enthalten.

Bei der nächsten Replikation entdeckt Kaspersky Anti-Virus die Objekte, erkennt sie als nicht desinfizierbar, und führt die Aktionen aus, die in den Einstellungen des Replikationsschutzes für solche Objekte ausgewählt sind (im Fall der Verwendung eines modifizierten Test-"viruses" – den verwendeten Präfixen entsprechend. Siehe Abschnitt "Test "virus" EICAR und seine Modifikationen" auf der S. 119). Standardmäßig wird ein nicht desinfizierbares Objekt gelöscht. Informationen über die Erkennung und der ausgeführten Aktion, werden in die Ereignisprotokoll- und Statistikdatenbank geschrieben. An Serveradministratoren oder Profiladministratoren , in dessen Bestand dieser Server enthalten ist, wird eine Warnungsmeldung gesendet.

Machen Sie sich mit der Statistik des Replikationsschutzes vertraut und prüfen Sie die an die Administratorenadresse eingegangene Meldungen.

TESTEN DER DATENBANKENUNTERSUCHUNG

Es wird empfohlen, die Virenerkennung in Rich Text Format Texten, Anhängen und OLE-Objekten zu überprüfen.

- *Um die Virenerkennung bei der Datenbankenuntersuchung zu überprüfen, gehen Sie wie folgt vor:*

1. Wählen Sie eine Datenbank auf dem geschützten Server, und wählen Sie dann ein Dokument aus, welches ein RTF-Feld enthält, oder Sie erstellen eine Datenbank aufgrund eines vorhandenen Templates, und erstellen Sie ein Dokument, das ein RTF-Feld enthält.
2. Platzieren Sie den Text des standardisierten oder modifizierten Test-"viruses" in das RTF-Feld des ausgewählten Dokuments.
3. Fügen Sie zum ausgewählten Dokument eine Datei oder ein OLE-Objekt hinzu, die den Text des standardisierten oder modifizierten Test-"viruses" enthalten.

Bei der nächsten Replikation entdeckt Kaspersky Anti-Virus die Objekte, erkennt sie als nicht desinfizierbar, und führt die Aktionen aus, die in den Einstellungen des Replikationsschutzes für solche Objekte ausgewählt sind (im Fall der Verwendung eines modifizierten Test-"viruses" – den verwendeten Präfixen entsprechend. Siehe Abschnitt "Test "virus" EICAR und seine Modifikationen" auf der S. 119). Standardmäßig wird ein nicht desinfizierbares Objekt gelöscht. Informationen über die Erkennung und der ausgeführten Aktion, werden in die Ereignisprotokoll- und Statistikdatenbank geschrieben. An Serveradministratoren oder Profiladministratoren , in dessen Bestand dieser Server enthalten ist, wird eine Warnungsmeldung gesendet.

Machen Sie sich mit der Statistik des Replikationsschutzes vertraut und prüfen Sie die an die Administratorenadresse eingegangene Meldungen.

SERVER-KONSOLE-MODUS

Sie können einige der Kaspersky Anti-Virus Hauptfunktionen durch die Befehlszeile des Domino-Servers verwalten. In diesem Abschnitt sind Systembefehle aufgezählt, die die Verwaltung der Kaspersky Anti-Virus Funktionen sichern.

Systembefehle werden nur für kavcontrol Aufgaben auf jedem einzelnen Server separat eingegeben.

Der Befehl muss folgende Syntax haben:

```
tell kavcontrol <Befehl> [<Parameter>]
```

wobei:

- `Befehl` – Befehl von Kaspersky Anti-Virus;
- `Parameter` – der für den Befehlsstart benötigte Parameter (wenn nötig).

Falls als Parameterwert ein Datei- oder Ordnerpfad angegeben wird, sollte man sich an die Regeln der Pfadbildung des am Server installierten Betriebssystems halten. Falls im Dateipfad ein Leerzeichen verwendet wird, muss der ganze Pfad durch doppelte Anführungszeichen eingeschlossen werden. Die Anführungszeichen dürfen nicht durch ein Leerzeichen vom Parameterwert abgesondert werden. Zwischen dem Parameter und dem Befehl muss ein Leerzeichen liegen.

Beispiel:

Korrekt:

```
tell kavcontrol addlicensekey "/home/petia/my key"
```

Inkorrekt:

```
tell kavcontrol addlicensekey " /home/petia/my key"
```

Die Liste von Kaspersky Anti-Virus Befehlen wird in der nachstehenden Tabelle angeführt.

Tabelle 7. Kaspersky Anti-Virus Befehle

BEFEHL	PARAMETER	AKTION
Help		Verfügbare befehle anzeigen.
AddLicenseKey	<vollständiger_Pfad_zur_Lizanzdatei_auf_dem_Server>	Lizenzdatei hinzufügen.
DelFirstKey		Aktiven Lizenzschlüssel löschen.
DelSecondKey		Zusätzlichen Aktivierungsschlüssel löschen.
ShowLicense		Information über die aktive Lizenz anzeigen.
StartScanner		Datenbankenuntersuchung starten.
StopScanner		Datenbankenüberprüfung beenden.
PauseScanner		Datenbankenüberprüfung anhalten.
ResumeScanner		Datenbankenüberprüfung fortsetzen.
StartUpdater		Update der Anti-Viren-Datenbanken starten.
StopUpdater		Update der Anti-Viren-Datenbanken beenden.
ShowVersion		Versionsnummer des auf dem Server installierten Kaspersky Anti-Viren Produktes anzeigen.

ANFRAGE AN DEN TECHNISCHEN SUPPORT

Falls Sie Kaspersky Anti-Virus bereits besorgt haben, können Sie Informationen über dieses Programm von den Spezialisten des technischen Supports per Telefon oder Internet erhalten.

Die Spezialisten des technischen Supports beantworten Ihre Fragen bezüglich der Programminstallation und -anwendung. Falls Ihr Computer infiziert wurde, helfen sie die Nachwirkungen der bösartigen Programme zu beheben.

Bevor Sie sich an den technischen Support zu wenden, machen Sie sich bitte mit den Support-Regeln vertraut (http://support.kaspersky.com/de/support/rules).

Elektronische Anfrage an den technischen Support

Sie können eine Frage an die Spezialisten des technischen Supports stellen, indem Sie das Web-Formular des Kundenanfragesystems Helpdesk ausfüllen (http://www.kasperskylab.de/2506--~de~1_startseite.html).

Um eine elektronische Anfrage zu senden, müssen Sie die **Kundennummer**, die Sie bei der Registrierung auf der Web-Seite des technischen Supports erhalten haben, sowie das **Kennwort** angeben.

Falls Sie noch kein registrierter Benutzer von Kaspersky Lab Programmen sind, können Sie das Registrierungsformular ausfüllen (https://support.kaspersky.com/ru/personalcabinet/Registration/Form/?LANG=de). Beim Registrieren geben Sie den *Aktivierungscode* des Programms oder den *Lizenzdateinamen* an.

Sie erhalten Antwort auf Ihre Anfrage von den Spezialisten des technischen Supports in Ihrem Persönlichen Cabinet (https://support.kaspersky.com/ru/personalcabinet?LANG=de) sowie an die der E-Mail-Adresse, die Sie in der Anfrage angegeben haben.

In dem Anfrage-Web-Formular beschreiben Sie das vorhandene Problem ausführlich. In den Pflichtfeldern geben Sie bitte folgendes an:

- **Anfragetyp**. Wählen Sie das Thema, das dem Problem am nächsten entspricht, beispielsweise, "Problem bei Produktinstallation/-deinstallation" oder "Problem bei Virensuche/-entfernung". Falls Sie kein passendes Thema finden, wählen Sie die "Allgemeine Frage".
- **Programmname und Versionsnummer**.
- **Anfragetext**. Beschreiben Sie das vorhandene Problem möglichst ausführlich.
- **Kundennummer und Kennwort**. Geben Sie die Kundennummer und das Kennwort ein, das Sie beim Registrieren auf der Web-Seite des technischen Supports erhalten haben.
- **E-Mail-Adresse**. An diese Adresse senden die Spezialisten des technischen Supports die Antwort auf Ihre Anfrage.

Technischer Support per Telefon

Falls das Problem dringend ist, können Sie den lokalen technischen Support anrufen. Vor der Anfrage an den technischen Support (http://support.kaspersky.com/de/support/international) sammeln Sie bitte alle Informationen (http://support.kaspersky.com/de/support/details) über Ihren Computer und über das installierte Virenschutzprogramm. Dies ermöglicht es unseren Spezialisten, Ihnen schneller zu helfen.

GLOSSAR

A

Abfänger(Interceptor)

Teilkomponente des Programms, die für die Überprüfung einzelner Typen der E-Mails verantwortlich ist. Abfänger werden je nach dem installiert, in welcher Rolle oder Rollenkombination das Programm installiert wurde.

Archiv

Eine Datei, die ein oder mehrere Objekte enthält, die wiederum Archive sein können.

I

Infiziertes Objekt

Ein Objekt, in dem ein bösartiger Code enthalten ist. Bei der Objektüberprüfung wurde eine vollständige Übereinstimmung des Objektcodes mit dem Code einer bekannten Bedrohung festgestellt. Spezialisten von Kaspersky Lab empfehlen Ihnen nicht, mit solchen Objekten weiter zu arbeiten, da es eine Infektion Ihres Computers nach sich ziehen kann.

M

Möglicherweise infiziertes Objekt

Ein Objekt, dessen Code entweder einen modifizierten Code eines bekannten Virus enthält oder einen Code, der einem Virus ähnlich ist, welcher Kaspersky Lab noch nicht bekannt ist. Möglicherweise infizierte Objekte werden mit Hilfe des heuristischen Analysators entdeckt.

O

OLE-Objekt

Hinzugefügtes oder in eine andere Datei eingebettetes Objekt. Das Kaspersky Lab Programm überprüft OLE-Objekte auf das Vorhandensein von Viren. Beispielsweise, falls Sie in eine Microsoft Office Excel Tabelle in ein Microsoft Office Word Dokument einfügen, wird diese Tabelle als OLE-Objekt überprüft.

Q

Quarantäne

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte, die bei der Überprüfung oder im Betrieb des Echtzeit Schutzes entdeckt wurden, gespeichert werden.

S

Schlüsseldatei

Ihr persönlicher Schlüssel mit der Dateiendung .key, der für den Betrieb von Kaspersky Lab Programm nötig ist. Die Schlüsseldatei ist im Lieferumfang des Produktes enthalten, wenn Sie sie über einen Lizenzdistributor von Kaspersky Lab bezogen haben oder wird Ihnen via E-Mail übermittelt, falls das Produkt im Online-Shop erworben wurde.

U

UPDATE DER DATENBANKEN

Eine Funktion, die von Kaspersky-Lab-Programmen ausgeführt wird und die es erlaubt den aktuellen Status des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von Kaspersky-Lab-Updateservern auf Ihren Computer kopiert und automatisch vom Programm verarbeitet.

UPDATE-PAKET

Datei-Paket für das Software-Update, welches vom Internet kopiert wird und auf Ihrem Computer installiert wird.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Die Firma ist heute das bekannteste Unternehmen für Datenschutz-Software in Russland und bietet eine breite Palette an IT-Sicherheitslösungen zum Schutz vor Viren, Spam und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Der Stammsitz befindet sich in Russland. Das Unternehmen unterhält Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Beneluxstaaten, in China, Polen, Rumänien und in den USA. In Frankreich wurde eine neue Filiale gegründet, das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk verbindet weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das ist heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome, sechzehn einen Doktortitel haben. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens besteht in dem einzigartigen Wissen und in der Erfahrung, die von den Mitarbeitern im Laufe des mehr als vierzehnjährigen kontinuierlichen Kampfes gegen Viren gesammelt wurden. Dank der permanenten Analyse von Virenaktivitäten sind wir in der Lage, Tendenzen in der Malware-Entwicklung zu prognostizieren und unseren Benutzern rechtzeitig zuverlässigen Schutz vor neuen Angriffen zu gewährleisten. Dieser Vorteil manifestiert sich in den Erzeugnissen und Leistungen von Kaspersky Lab. Wir sind unseren Konkurrenten stets einen Schritt voraus und bieten unseren Kunden Schutz von höchster Güte.

Aufgrund der jahrelangen Tätigkeit ist das Unternehmen jetzt ein führender Entwickler im Bereich der Virenschutztechnologien. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Das Basisprodukt des Unternehmens heißt Kaspersky Anti-Virus®. Es bietet für alle Arten von Objekten zuverlässigen Schutz vor Virenangriffen: Arbeitsstationen, Dateiserver, Mailsysteme, Firewalls und Internet-Gateways, Handhelds. Bequeme Steuerelemente erlauben es dem Benutzer, den Antivirenschutz von Computern und Firmennetzwerken möglichst weitgehend zu automatisieren. Viele Entwickler auf der ganzen Welt verwenden in ihrer Software den Kern vom Kaspersky Anti-Virus®. Zu ihnen gehören u.a.: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir planen, realisieren und begleiten komplexe Antivirenlösungen für Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Rund um die Uhr steht unseren Benutzern ein technischer Kundendienst in mehreren Sprachen zur Verfügung.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gerne telefonisch oder per E-Mail beraten. Alle Ihre Fragen werden umfassend beantwortet.

Webseite von Kaspersky Lab:	www.kaspersky.de
Viren-Enzyklopädie:	http://www.viruslist.com/de/
Anti-Viren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalysten)

INFORMATIONEN ZU VERWENDETEN FREMDEN CODES

Beim Programmerstellen wurde der Code der Fremdhersteller verwendet.

IN DIESEM ABSCHNITT

Programmcode 128

Entwicklungsmittel 141

Sonstige Informationen 145

PROGRAMMCODE

Information über den Programmcode der Fremdhersteller, der beim Programmerstellen verwendet wurde.

BOOST 1.30

Copyright (C) 2003, Christof Meerwald

EXPAT 1.2

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GECKO SDK 1.8

Copyright (C) 1998-2008, Mozilla Foundation

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use"

means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor"

means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version"

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code"

means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work"

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License"

means this document.

1.8.1. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications"

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code"

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims"

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code"

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of

any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.auf der S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.auf der S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of

Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS"

basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the

License for the specific language governing rights and limitations

under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms

of the _____ license (the "[___] License"), in which case the

provisions of [_____] License are applicable instead of those

above. If you wish to allow use of your version of this file only

under the terms of the [____] License and not to allow others to use

your version of this file under the MPL, indicate your decision by

deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete

the provisions above, a recipient may use your version of this file

under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments,

including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape

Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator

client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape

lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original

Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code.

To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may

choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if

such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public

License Version 1.1 (the "License"); you may not use this file

except in compliance with the License. You may obtain a copy of

the License at http://www.mozilla.org/NPL/

Software distributed under the License is distributed on an "AS

IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or

implied. See the License for the specific language governing

rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released

March 31, 1998.

The Initial Developer of the Original Code is Netscape

Communications Corporation. Portions created by Netscape are

Copyright (C) 1998-1999 Netscape Communications Corporation. All

Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the

terms of the _____ license (the "[___] License"), in which case

the provisions of [_____] License are applicable instead of

those above. If you wish to allow use of your version of this

file only under the terms of the [____] License and not to allow

others to use your version of this file under the NPL, indicate

your decision by deleting the provisions above and replace them

with the notice and other provisions required by the [___]

License. If you do not delete the provisions above, a recipient

may use your version of this file under either the NPL or the

[___] License."

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

Info-ZIP license

This is version 2007-Mar-4 of the Info-ZIP license.

The definitive version of this document should be available at

ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely and

a copy at http://www.info-zip.org/pub/infozip/license.html.

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including,

but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip, "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

LZMA SDK 4.43

OPENSSL 0.9.8D

Copyright (C) 1998-2007, The OpenSSL Project

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY O

SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

PCRE 7.4

Copyright (C) 1997-2008, University of Cambridge

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service, Cambridge, England.

Copyright (c) 1997-2007 University of Cambridge

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

ZLIB 1.2

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

ENTWICKLUNGSMITTEL

Informationen über Entwicklungstools und andere Tools und Mittel von Drittherstellern, die bei der Programmentwicklung verwendet wurden.

AUTOCONF 2.61

Copyright (C) 1992, 1993, 1994, 1998, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

AUTOMAKE 1.10

Copyright (C) 1994, 1995, 1996, 1997, 1998, 2001, 2003, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

AWK 3.1.5

Copyright (C) 1986, 1988, 1989, 1991-2005, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

BASH 3.2.33

Copyright (C) 1989-2005, Free Software Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 3 of the License

GCC 4.1.2

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GCC 3.4.5

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GCC 3.3.6

Copyright (C) 1987, 1989, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GCC 3.3.2

Copyright (C) 1999, 2000, 2001, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

Distributed under the terms of the [GNU] Lesser General Public License as published by the Free Software Foundation, version 2.1 of the License

GNU MAKE 3.81

Copyright (C) 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Free Software

Foundation, Inc

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

GREP 2.5.1

Copyright 1992, 1997-1999, 2000, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

PERL 5.8.8

Copyright (C) 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, Larry Wall and others

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 1 of the License

=======

The "Artistic License"

Preamble

The intent of this document is to state the conditions under which a Package may be copied, such that the Copyright Holder maintains some semblance of artistic control over the development of the package, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

Definitions:

"Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder as specified below.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide a separate manual page for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) give non-standard executables non-standard names, and clearly document the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you do not advertise this Package as a product of your own. You may embed this Package's interpreter within an executable of yours (by linking); this shall be construed as a mere form of aggregation, provided that the complete Standard Version of the interpreter is so embedded.

6. The scripts and library files supplied as input to or produced as output from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whoever generated them, and may be sold commercially, and may be aggregated with this Package. If such scripts or library files are aggregated with this Package via the so-called "undump" or "unexec" methods of producing a binary executable image, then distribution of such an image shall neither be construed as a distribution of this Package nor shall it fall under the restrictions of Paragraphs 3 and 4, provided that you do not represent such an executable image as a Standard Version of this Package.

7. C subroutines (or comparably compiled subroutines in other languages) supplied by you and linked into this Package in order to emulate subroutines and variables of the language defined by this Package shall not be considered part of this Package, but are the equivalent of input as in Paragraph 6, provided these subroutines do not change the language in any way that would cause it to fail the regression tests for the language.

8. Aggregation of this Package with a commercial distribution is always permitted provided that the use of this Package is embedded; that is, when no overt attempt is made to make this Package's interfaces visible to the end user of the commercial distribution. Such use shall not be construed as a distribution of this Package.

9. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

10. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

SED 4.1.5

Copyright (C)1989, 1990, 1991, 1992, 1993, 1994, 1995, 1998, 1999, 2002, 2003, Free Software Foundation, Inc

---

Distributed under the terms of the [GNU] General Public License as published by the Free Software Foundation, version 2 of the License

SONSTIGE INFORMATIONEN

Zusätzliche Informationen über den Fremdcode.

Zur Überprüfung der elektronischen digitalen Signatur wird die Programmbibliothek für den Informationsschutz (PBSI) "Agava-C" eingesetzt, die von R-Alpha OOO entwickelt wurde.

Die Software kann Software-Programme enthalten, für die der Nutzer eine (Unter-) Lizenz gemäß der GNU General Public License (GPL) bzw. ähnliche kostenlose Software-Lizenzen erhalten hat, die den Nutzer unter anderem dazu berechtigen, bestimmte Programme oder Teile davon zu kopieren, zu ändern und weiterzugeben und die den Zugang zum Quellcode gestatten ("Open Source Software"). Sofern diese Lizenzen erfordern, dass der Quellcode für eine in einem ausführbaren, binären Format weitergegebene Software dem Nutzer ebenfalls zugänglich gemacht wird, wird der Quellcode nach einer entsprechenden Anforderung an source@kaspersky.com zur Verfügung gestellt bzw. mit der Software geliefert.

GNU GENERAL PUBLIC LICENSE

=======

GNU GENERAL PUBLIC LICENSE

Version 1, February 1989

Copyright (C) 1989 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The license agreements of most software companies try to keep users at the mercy of those companies. By contrast, our General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. The General Public License applies to the Free Software Foundation's software and to any other program whose authors commit to using it. You can use it for your programs, too.

When we speak of free software, we are referring to freedom, not price. Specifically, the General Public License is designed to make sure that you have the freedom to give away or sell copies of free software, that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of a such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must tell them their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any work containing the Program or a portion of it, either verbatim or with modifications. Each licensee is addressed as "you".

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this General Public License and to the absence of any warranty; and give any other recipients of the Program a copy of this General Public License along with the Program. You may charge a fee for the physical act of transferring a copy.

2. You may modify your copy or copies of the Program or any portion of it, and copy and distribute such modifications under the terms of Paragraph 1 above, provided that you also do the following:

a) cause the modified files to carry prominent notices stating that you changed the files and the date of any change; and

b) cause the whole of any work that you distribute or publish, that in whole or in part contains the Program or any part thereof, either with or without modifications, to be licensed at no charge to all third parties under the terms of this General Public License (except that you may choose to grant warranty protection to some or all third parties, at your option).

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the simplest and most usual way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this General Public License.

d) You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

Mere aggregation of another independent work with the Program (or its derivative) on a volume of a storage or distribution medium does not bring the other work under the scope of these terms.

3. You may copy and distribute the Program (or a portion or derivative of it, under Paragraph 2) in object code or executable form under the terms of Paragraphs 1 and 2 above provided that you also do one of the following:

a) accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Paragraphs 1 and 2 above; or,

b) accompany it with a written offer, valid for at least three years, to give any third party free (except for a nominal charge for the cost of distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Paragraphs 1 and 2 above; or,

c) accompany it with the information you received as to where the corresponding source code may be obtained. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form alone.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable file, complete source code means all the source code for all modules it contains; but, as a special exception, it need not include source code for modules which are standard libraries that accompany the operating system on which the executable file runs, or for standard header files or definitions files that accompany that operating system.

4. You may not copy, modify, sublicense, distribute or transfer the Program except as expressly provided under this General Public License. Any attempt otherwise to copy, modify, sublicense, distribute or transfer the Program is void, and will automatically terminate your rights to use the Program under this License. However, parties who have received copies, or rights to use copies, from you under this General Public License will not have their licenses terminated so long as such parties remain in full compliance.

5. By copying, distributing or modifying the Program (or any work based on the Program) you indicate your acceptance of this license to do so, and all its terms and conditions.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of the license which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the license, you may choose any version ever published by the Free Software Foundation.

8. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

9. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

10. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to humanity, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 1, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19xx name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (a program to direct compilers to make passes at assemblers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

That's all there is to it!

=======

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details

type `show w'. This is free software, and you are welcome

to redistribute it under certain conditions; type `show c'

for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written

by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

=======

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the

GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no

warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that

this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits

relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author>

This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it

under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

=======

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its

contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.

Copyright (C) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either

version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

=======

SACHREGISTER

I

Infiziertes Objekt 125

K

KASPERSKY LAB 127

L

Lizenz 125
Erhalten von der Schlüsseldatei 125

V

Virenschutz 22